HP Client Automation

带外管理

适用于 Windows® 操作系统

软件版本：8.10

用户指南

文档发行日期：2012 年 2 月
软件发行日期：2012 年 2 月

法律声明

担保

HP 产品和服务的唯一担保已在此类产品和服务随附的明示担保声明中提出。此处的任何内容均不构成额外担保。HP 不会为此处出现的技术或编辑错误或遗漏承担任何责任。

此处所含信息如有更改，恕不另行通知。

受限权利声明

机密计算机软件。必须拥有 HP 授予的有效许可证，方可拥有、使用或复制本软件。按照 FAR 12.211 和 12.212，并根据供应商的标准商业许可的规定，商业计算机软件、计算机软件文档与商品技术数据授权给美国政府使用。

版权声明

© Copyright 2003-2011 Hewlett-Packard Development Company, L.P.

商标声明

Intel® 是 Intel Corporation 在美国和其他国家 / 地区的商标。

Java 是 Oracle Corporation 和 / 或其隶属公司的注册商标。

Microsoft®、 Windows®、 Windows® XP 和 Windows Vista® 是 Microsoft Corporation 在美国的注册商标。

致谢

本产品包含由 Apache Software Foundation (http://www.apache.org/) 开发的软件。

本产品包含由 Eric Young (eay@cryptsoft.com) 编写的加密软件。

本产品包含由 OpenSSL Project 开发的用于 OpenSSL Toolkit (http://www.openssl.org/) 的软件。

本产品包含由 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

文档更新

本文档的标题页包含以下标识信息：

- 软件版本号，用于指示软件版本。
- 文档发行日期，该日期将在每次更新文档时更改。
- 软件发布日期，用于指示该版本软件的发布日期。

要检查是否有最新的更新，或者验证是否正在使用最新版本的文档，请访问：

http://h20230.www2.hp.com/selfsolve/manuals

需要注册 HP Passport 才能登录此站点。要注册 HP Passport ID，请访问：

http://h20229.www2.hp.com/passport-registration.html

或单击 “HP Passport”登录页面上的 “New users - please register”链接。

此外，如果订阅了相应的产品支持服务，则还会收到更新的版本或新版本。有关详细信息，请与您的 HP 销售代表联系。

支持

访问 HP Software 联机支持网站，网址为：

www.hp.com/go/hpsoftwaresupport

该网站提供联系信息，以及有关 HP Software 所提供的产品、服务和支持的详细信息。

HP Software 联机支持可协助客户自行解决问题。该联机支持提供了一种访问业务管理所需的交互技术支持工具的快速有效的方法。作为我们的尊贵客户，您可以通过该支持网站获得下列支持：

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件修补程序
- 管理支持合同
- 查找 HP 支持联系信息
- 查看有关可用服务的信息
- 参与其他软件客户的讨论
- 研究和注册软件培训

大多数提供支持的区域都要求您注册为 HP Passport 用户再登录，很多区域还要求用户提供支持合同。要注册 HP Passport 用户 ID，请访问：

http://h20229.www2.hp.com/passport-registration.html

要查找有关访问级别的详细信息，请访问：

http://h20230.www2.hp.com/new_access_levels.jsp

目录

1 简介 9
概述 9
缩写和变量 10
OOBM 工作流程 10
HPCA 中的 OOBM 结构 11
OOBM 管理操作 12
OOBM 的优势 14

2 设置 vPro 和 DASH 设备 15
设置 vPro 设备 16
vPro 设备的 SCS 置备 16
不同系统上的 HPCA 和 SCS 16
设置 TLS 模式 16
设置 SCS Server 22
安装 “设置与配置服务” 22
登录到 SCS Console 22
配置 SCS 服务设置 22
创建和配置配置文件 22
置备 vPro 设备 23
使用 MEBx 配置 vPro 设备 24
使用远程配置配置 vPro 设备 24
查看 vPro 设备 29
更改验证模式 29
设置 DASH 设备 30
DASH 配置 30
DASH 配置实用程序 31

3 OOBM 配置 33
配置参数信息 33
重新配置 SCS 路径 33
重新配置 Client Automation Web 服务 33
配置 IDE-R 驱动器 33
配置 SOL 端口 34
配置 SNMP 端口 34
配置 IDE-R 和 SOL 超时值 34
配置 Web 服务超时值 34
配置 DASH 设备的缓存大小 35
配置安全参数 35
配置监视程序设置 36
用于调试的配置设置 36

设置配置参数 36
配置 OOBM 服务和 SCS 之间的安全访问 45
禁用 OOBM 服务和 SCS 之间的安全访问 45
将根证书导入 Java 密钥库 46
将证书转换成 PEM 格式 47

4 管理任务 49
启用 49
配置 49
操作 50
管理 50
Client Automation Enterprise 50
Client Automation Standard 51
设备类型选择 52
通过设备类型选择确定配置和操作选项 53
vPro 系统防御设置 53
管理系统防御过滤器 54
管理系统防御策略 57
管理启发信息 61
管理监视程序 64
执行置备任务 69

5 设备管理 73
管理多个设备 73
设备发现 74
多个设备选择 76
DASH 设备管理的凭据 76
刷新设备信息 77
电源管理 78
警告订阅管理 78
常见实用程序的管理 78
系统防御策略的部署 79
启发的部署 80
监视程序的部署 80
代理程序软件列表和系统消息的部署 81
删除设备 81
管理单个设备 82
查看电源状态 82
查看 vPro 事件日志 87
查看 vPro 事件过滤器 87
查看 vPro 常规资产信息 88
查看硬件资产 88
查看软件资产 89
更改电源状态 90
重新启动系统 94
重新启动带 IDE-R 的 vPro 系统 95
重新启动 vPro 系统至 BIOS 设置 97

重新启动系统以预引导执行环境 99
引导至仅支持 DASH 的电源状态 100
vPro 设备上的 KVM 重定向 101
管理 vPro 设备上的系统防御过滤器 102
管理 vPro 设备上的系统防御策略 103
管理 vPro 设备上的启发 105
管理 vPro 设备上的监视程序 106
配置 vPro 设备上的前面板设置 107
重置 vPro 设备上的闪存限制 107
配置 vPro 设备上的引导设置 108

6 组管理 111
管理多个 vPro 设备组 111
多个组选择 112
同步组列表与 Client Automation 储备库 112
电源管理 113
警告订阅管理 113
OOBM 代理程序软件列表的部署 113
置备 114
系统防御策略的部署 114
监视程序的部署 115
启发的部署 116
管理单个 vPro 设备 117
“常规”选项卡 117
“属性”选项卡 117
“设备”选项卡 117

7 警告通知 119
查看 vPro 设备上的警告 119

8 用例方案 121
硬件故障和更换 121
概述 121
用例步骤 122
操作系统故障和重新引导 122
概述 123
用例步骤 123
病毒感染检测和隔离 123
概述 124
用例步骤 124
设备隔离和修复 126
概述 126
用例步骤 126
监视关键软件 128
概述 128
用例步骤 129
蠕虫病毒感染和控制 134
概述 134
用例步骤 134

9 疑难解答 137
常见问题 137
常规 138
置备 143
发现 144
远程操作 147
电源状态 153
重新启动 154
系统防御和代理程序存在 157
无线 162
迁移问题 163
备份 OOBM 数据 164
配置文件 164
数据文件 165
数据库 165
端口信息摘要 165
清单问题 166

A OOBM 功能 167
发现 167
硬件资产 167
软件资产 167
修复 168
远程操作 168
事件管理 169
保护 170
系统防御 170
代理程序存在 172
启发式网络病毒爆发控制 174

B vPro 设备的延迟远程配置 177
转换为设置模式 177
远程配置置备过程 178
通过 HPCA Console 的延迟远程配置 179

C 可信证书 181
可信证书 181
TLS 服务器验证 181
TLS 相互验证 182

1 简介

概述

借助 HP Client Automation (HPCA) Server，无论系统电源或操作系统如何，您都可以使用带外管理 (OOBM) 功能执行带外操作。

带内管理是指在启动具有运行中操作系统的计算机时执行的操作。

带外管理是指计算机处于以下任一状态时执行的操作：

- 计算机的电源已接通，但没有运行 （关闭、待机、休眠）。
- 未加载操作系统 （软件或引导故障）。
- 基于软件的管理代理程序不可用。

HPCA Server 支持对 Intel vPro 设备和已启用 DASH 的设备进行带外管理。

Intel vPro 设备即使在关闭时也可以被发现和管理，因为 Intel Active Management Technology (AMT) 固件在非易失性内存中存储有设备信息，并提供了一组可通过远程管理控制台调用的管理操作。DASH 是多个分布式管理任务组 (DMTF) 管理方案之一，提供管理计算机系统所需的，独立于计算机状态、操作平台或供应商的综合语法和语义框架。

上述两种技术都具有远程诊断和修复功能，包括基于硬件的远程引导和文本控制台重定向。

有关 Intel vPro 和 DASH 设备的详细信息，请参见第 2 章，设置 vPro 和 DASH 设备。

通过 OOBM 功能可以在 HPCA 环境中使用设备的一些进程，例如发现进程、修复进程和保护进程。

- 发现
  OOBM 使您能够在环境中标识硬件和软件资产。这有助于确定设备硬件规范、标识设备应用程序、解决兼容问题等等。
- 修复
  OOBM 利用诸如“远程操作”和“事件管理”这样的操作以帮助确定、诊断和修复任何软件、操作系统及硬件故障。事件管理功能只适用于 vPro 设备。
- 保护
  OOBM 只能帮助您保护 vPro 设备不受恶意软件和蠕虫病毒繁殖的侵害。它会监视在设备上运行的代理程序，以便在网络中隔离蠕虫病毒感染的设备。

有关发现、修复和保护进程的详细信息，请参见附录 A， OOBM 功能。

缩写和变量

本指南使用下表中定义的缩写形式和变量。

表 1　本指南中使用的缩写形式

缩写	定义
HPCA	HP Client Automation
Core 和 Satellite	由一个 Core Server 和一个或多个 Satellite Server 组成的 HPCA Enterprise 环境。所有功能都作为 Core 或 Satellite Server 安装的一部分。
CSDB	Configuration Server Database
Portal	HPCA Portal

表 2　本指南中使用的变量

变量	描述	默认值
InstallDir	安装 HPCA Server 的位置	32 位操作系统：`C:\Program Files\Hewlett-Packard\HPCA` 64 位操作系统：`C:\Program Files(x86)\Hewlett-Packard\HPCA`
SystemDrive	安装了 HPCA Server 的驱动器的盘符	`C:`

OOBM 工作流程

本节介绍了要在 HPCA 环境中成功实施 OOBM 需要采取的步骤。

1 **标识并设置设备**
这是使用 OOBM 的先决条件。在开始使用 OOBM 之前，需要标识并设置 Intel vPro 和已启用 DASH 的设备。另外，需要配置 SCS Server 以与 vPro 设备通信。有关设置和配置 SCS Server、Intel vPro 设备和已启用 DASH 的设备的详细信息，请参见第 2 章，设置 vPro 和 DASH 设备。

2 **在 HPCA 环境中启用 OOBM**

可通过使用 HPCA Server 完成此操作。在 HPCA Server 中启用 OOBM 以管理 Intel vPro 设备和已启用 DASH 的设备。有关详细信息，请参见第 4 章，管理任务。

3 **配置 OOBM （可选）**

这是可选任务。如果要更改 OOBM 中的默认设置，可以使用配置参数在 HPCA 环境中配置 OOBM。有关配置 OOBM 的详细信息，请参见第 3 章， OOBM 配置。

4 **执行管理任务**

启用 OOBM 后，可以执行的任务包括选择设备类型、设置 vPro 系统防御、置备 vPro 设备及其他管理任务。有关详细信息，请参见第 4 章，管理任务。

5 **管理设备**

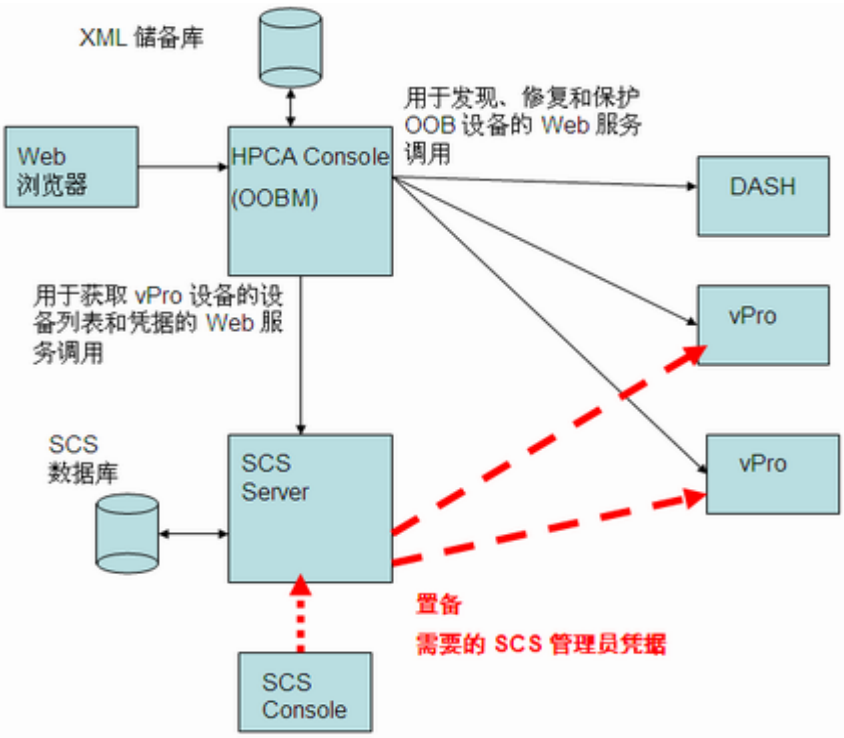
可以通过作为管理员或操作员在 HPCA Server 的 “操作”选项卡上执行以下任务，来开始管理设备：

- **管理设备**：“设备管理”选项允许您管理多个和单个 OOB 设备。这些任务包括刷新数据、重新加载设备信息、发现设备、开启 / 关闭和重新启动设备、订阅 / 取消订阅 vPro 警告、管理 vPro 设备上的常见实用程序，等等。有关详细信息，请参见第 5 章，设备管理。
- **管理组**：使用“组管理”选项可管理在 Client Automation 软件中定义的 vPro 设备组。可以在包含 vPro 设备的 Client Automation 组上执行 OOB 操作。可以管理多个 vPro 设备组，以执行不同的发现、修复和保护任务。这些任务包括电源管理、警告订阅和部署系统防御策略、监视程序、 OOBM 代理程序软件列表和启发。有关详细信息，请参见第 6 章，组管理。
- **查看警告**：对于 vPro 设备，只要您有该设备的警告订阅，就可以查看由已置备的 vPro 设备生成的警告。监视警告通知可使您了解网络上设备的运行状况。有关详细信息，请参见第 7 章，警告通知。

HPCA 中的 OOBM 结构

下图说明了 OOBM 中的结构和通信接口。

图 1　带外管理结构



OOBM 管理操作

下表总结了根据要管理的 OOB 设备类型，可用的管理操作。

表 3　带外设备上的管理操作

管理操作	vPro	DASH	何处查找信息
置备配置 *	X		执行置备任务 （第 69 页）
设备发现 **	X	X	设备发现 （第 74 页）
管理多个设备	X	X	管理多个设备 （第 73 页）
常规资产发现	X		查看 vPro 常规资产信息 （第 88 页）
硬件资产发现	X	X	查看硬件资产 （第 88 页）
软件资产发现 ***	X	X	查看软件资产 （第 89 页）
电源管理 ****	X	X	更改电源状态 （第 90 页）
重新启动 ****	X	X	重新启动系统 （第 94 页）

表 3　带外设备上的管理操作 （续）

管理操作	vPro	DASH	何处查找信息
用 IDE-R 重新启动 ****	X		重新启动带 IDE-R 的 vPro 系统 （第 95 页）
重新启动至 BIOS****	X		重新启动 vPro 系统至 BIOS 设置 （第 97 页）
重新启动至 LAN (PXE)****	X	X	重新启动系统以预引导执行环境 （第 99 页）
重新启动或启动至更离散的休眠状态 ****		X	引导至仅支持 DASH 的电源状态 （第 100 页）
文本控制台重定向	X	X	远程操作 （第 168 页）
设备组管理	X		组管理 （第 111 页）
事件管理	X		查看 vPro 事件日志 （第 87 页），查看 vPro 事件过滤器 （第 87 页），警告通知 （第 119 页）
系统防御	X		管理系统防御过滤器 （第 54 页），管理系统防御策略 （第 57 页）
代理程序存在	X		管理监视程序 （第 64 页）
启发蠕虫病毒控制	X		管理启发信息 （第 61 页）
前面板设置配置	X		配置 vPro 设备上的前面板设置 （第 107 页）
闪存限制重置	X		重置 vPro 设备上的闪存限制 （第 107 页）
引导设置配置		X	配置 vPro 设备上的引导设置 （第 108 页）
删除设备	X	X	删除设备 （第 81 页）

* 置备配置：可使用多种方式置备 vPro 设备。 HPCA Server 仅代表通过延迟远程配置而实现的一种方式。假定 DASH 设备已按照计算机文档置备。

** 设备发现：用 SCS 设备储备库发现 vPro 设备。通过指定 IP 地址或 Active Directory (AD) 发现 DASH 设备。

*** 软件资产发现：用位于第三方数据存储中的信息，发现 vPro 设备上的软件资产。在 DASH 设备上，用位于网络控制器的 NVRAM 中的信息发现它们。

**** 电源和重新启动操作：请参见表 13 （第 84 页）。

OOBM 的优势

HPCA Server 中的 OOBM 具有几点优势。下面列出这些优势：

- 如果计算机具有 vPro 技术或通过实施 DASH 标准变得可访问，则即使计算机关闭、操作系统未运行或缺少管理代理程序，也可利用基于硬件的管理功能。
- 提高从最初部署到租赁协议终止的硬件和软件库存的准确性和完全性。
- 减少桌面端访问的需求，因为计算机可以远程开机、重新启动和重新映像。
- 为 vPro 设备提供系统防御功能，以便根据 HPCA Server 上创建的策略和过滤器有选择地对 Ethernet 和 IP 协议数据包流量进行网络隔离。
- 提供代理程序存在功能，通过从 HPCA Server 中创建的监视程序可对 vPro 系统上运行的 OOBM 代理程序进行监视。如果受监视的代理程序停止运行，则启用代理程序存在策略和 / 或记录事件。
- 为 vPro 设备提供独立于操作系统、防篡改的蠕虫病毒控制系统。检测到蠕虫时，隔离主机并向 HPCA Server 发送通知。
- 通过 HTTP 验证和运行在被管 vPro 设备操作系统层之下的传输层安全 (TLS)，提供安全、始终可用的通信通道。

2 设置 vPro 和 DASH 设备

Intel vPro 设备通过 Intel 活动管理技术 (AMT) 来实现。AMT 只是 vPro 技术的一部分。Intel 芯片组和 Intel 网络接口卡 (NIC) 也是 vPro 技术解决方案的一部分。Intel vPro 设备即使在关闭时也可以被发现和管理，因为 Intel AMT 固件是将设备信息存储在非易失性内存中，并提供一组可通过远程管理控制台调用的管理操作。

同样，已启用 DASH 的设备也可以利用带外管理。 DASH 旨在为桌面和移动系统的安全带外管理和远程管理提供新一代标准。DASH 是多个分布式管理任务组 (DMTF) 管理方案之一，提供管理计算机系统所需的，独立于计算机状态、操作平台或供应商的综合语法和语义框架。

上述两种技术都具有远程诊断和修复功能，包括基于硬件的远程引导和文本控制台重定向。在 vPro 设备上，通过电子集成驱动器重定向 (IDE-R) 提供远程引导，通过 serial over LAN (SOL) 技术提供文本控制台重定向。

Intel vPro 技术还支持自动置备远程 vPro 设备。此外，它还提供系统防御和代理程序存在能力，用以保护 vPro 设备免受恶意软件攻击和，保证不删除保护系统的 OOBM 代理程序。而且，它还提供网络爆发遏制 (NOC) 启发机制，用于测量、分析和应对流量以检测并阻止蠕虫病毒繁殖。

所有 vPro OOBM 功能都受 Transport Layer Security (TLS) 和 Digest 验证保护。对于已启用 DASH 的设备，目前唯一支持的机制是 Digest 验证。

- HPCA Server 不支持 Kerberos 验证。
- 发现和管理 OOB 设备的唯一条件是，设备实际地接入网络并接通电源。

设置 vPro 设备

要使 vPro 设备正常运行， SCS Server （也称为 “设置与配置服务器”）需要执行所有必需步骤。SCS Server 是运行 Intel 设置与配置服务 (SCS) 的系统，并且仅与 vPro 设备相关。

要让 SCS Server 和 vPro 设备相互通信，必须在通信的两端执行以下各节所述的设置与配置步骤。

➤ 确保使用与位于 `Media\OOBM\win32\AMT Config Server` 目录中的 HPCA Core 分发介质捆绑的 SCS 软件版本。而且，如果正在从较早版本迁移，请确保也将 SCS 软件迁移到分发介质上所含的当前版本。否则，可能遇到错误行为。

vPro 设备的 SCS 置备

SCS Server 和 vPro 设备安全地通信。SCS Server 将生成 vPro 设备初始参数值和安全性相关配置信息，并将其发送。设置与配置内包括设置配置文件中包含的参数或自动生成的参数。

有关与 vPro 安全性相关的配置信息的详细信息，请参见位于 HPCA Core 分发介质的 `Media\oobm\win32\AMT Config Server` 目录中的 《Intel 设置与配置服务控制台用户指南 V5.4》 (Intel Setup and Configuration Service Console User Guide Version 5.4) 中的 “Intel SCS 简介 (Introduction to Intel SCS)” 一节。

有关设置与配置参数的详细信息，请参见 《Intel 设置与配置服务控制台用户指南 V5.4》 (Intel Setup and Configuration Service Console User Guide Version 5.4) 中的 “设置与配置操作概述 (Setup and Configuration Operational Overview)” 一节。

不同系统上的 HPCA 和 SCS

由于 SCS 和 HPCA 的支持操作系统平台可能不同，可能需要将 SCS 软件和 HPCA 软件安装到单独的系统上。

设置 TLS 模式

如果不需要 TLS，则跳到设置 SCS Server （第 22 页）。

安全性对于许多 vPro 功能非常重要，尤其是重定向功能。serial over LAN (SOL) 和驱动器电子重定向 (IDE-R) 的使用模型包括允许远程诊断、引导和操作系统安装的远程故障诊断。这些过程通常涉及验证步骤，此步骤要求将用户名和密码作为重定向会话的一部分通过 LAN 发送。如果 vPro 设备支持 TLS，则在打开 SOL 或 IDE-R 会话之前，HPCA Server 将与其建立 TLS 会话，从而确保所有相关网络通信都是安全的。

必须对 vPro 设备使用相互验证，对 SCS Server 使用服务器验证。

➤ 如果在 HPCA Server 上设置 TLS 验证，则它仅能管理已配置为使用 TLS 的那些 vPro 设备。相反地，如果尚未在 HPCA Server 上设置 TLS 验证，则它仅能管理未配置为使用 TLS 的那些 vPro 设备。

执行以下任务来设置 TLS 模式：

任务 1： 安装 Microsoft Certification Authority

Microsoft Certification Authority 允许创建客户端证书以及导出客户端证书和可信根证书，以供用于 TLS 验证。

要在 Windows Server 2003 上安装 Microsoft CA，请执行以下步骤：

➤ 用于安装 Microsoft CA 的步骤可能随平台的不同而有所变化。

1. 单击 Windows **开始**按钮，并选择**控制面板**。
2. 双击**添加或删除程序**。
3. 从左面板中，单击**添加 / 删除 Windows 组件**。
4. 选中**证书服务**复选框。将显示一条警告消息，指示计算机充当证书服务器时，其计算机名称或域成员身份无法更改。单击**是**以关闭消息窗口。
5. 单击**详细信息**。
6. 选中**证书服务 CA** 复选框和**证书服务 Web 注册支持**复选框以指定证书服务的子组件。单击**确定**。
7. 在 “Windows 组件” 窗口上，单击**下一步**。此时将打开 “CA 类型” 窗口。
8. 选择 **Enterprise Root CA** 作为要设置的证书类型。单击**下一步**。此时将打开 “CA 标识信息” 对话框。
9. 在 “CA 标识信息” 对话框中，指定以下内容：
   - **此 CA 的公共名称**：Microsoft CA 的公共名称必须与正在安装 Microsoft CA 的计算机的名称相同。
   - **判别名后缀**：例如 **DC=AMT,DC=HP,DC=COM**
10. 完成 “Windows 组件设置向导” 中剩余的步骤。完成时，单击 “完成”。

这将安装 Microsoft CA 软件。 Microsoft CA 允许创建客户端证书（如以下各节所述）以及导出用于在验证过程中签名的可信根证书。导出过程如导出根证书 （第 20 页）中所述。

任务 2： 在 SCS Server 上创建 Internet Information Services 服务器证书

您必须具有服务器证书，以提供 SCS Server 和 SCS Console 之间的安全通信。

有关详细步骤，请参见位于 HPCA Core 分发介质的 `Media\oobm\win32\AMT Config Server` 目录中的《Intel 设置与配置服务安装指南 V5.4》(Intel Setup and Configuration Service Installation Guide Version 5.4) 中的 “安装 Microsoft Certification Authority (Installing Microsoft's Certification Authority)” 一章下的 “使用 SSL 保护到 IIS 的连接 (Securing the Connection to IIS Using SSL)” 一节。

任务 3： 创建客户端证书模板

必须为将在 HPCA Server 上安装的 TLS 相互验证创建客户端证书。

要创建客户端证书模板，请执行以下步骤：

1 单击 Windows **开始**按钮，并选择**运行**。

2 输入 **MMC**，并单击**确定**。此时将打开 Microsoft Management Console。

3 从 “文件” 菜单中，选择**添加 / 删除管理单元**。

4 单击**添加**。此时将打开 “添加独立管理单元” 对话框。

5 选择**证书模板**，并单击**添加**，然后单击**关闭**。

6 在 “添加 / 删除管理单元” 窗口中单击**确定**。

7 在左窗格中单击**证书模板**。所有现有模板都显示在控制台的右窗格中。

8 右键单击 “Web 服务器模板”，并选择**复制模板**。

9 在**常规**选项卡上，指定以下内容：

— **模板显示名称**：希望显示模板时出现的名称。例如，它可以是 `ClientAuthTmpl`。

— **模板名称**：模板的名称。它可以与显示名称相同。

— 选中**在 Active Directory 中发布证书**复选框。

10 在**正在处理的请求**选项卡上，选中**允许导出私钥**复选框。

11 在**扩展**选项卡上，选择**应用程序策略**，并单击**编辑**。此时将打开 “编辑应用程序策略扩展” 窗口。默认情况下显示服务器验证策略。

12 选择**服务器验证策略**，并单击**删除**。现在应用程序策略列表为空。

13 单击**添加**。此时将打开 “添加应用程序策略” 窗口。

14 在 “添加应用程序策略” 窗口中，选择**客户端验证策略**，并单击**确定**。“添加应用程序策略” 窗口关闭，并且此时将打开 “编辑应用程序策略扩展” 窗口。在列表中显示 “客户端验证策略”。

15 在 “编辑应用程序策略扩展” 窗口中，单击**添加**。此时将打开 “添加应用程序” 窗口。

16 单击**新建**。此时将打开 “新建应用程序策略” 窗口。

17 输入策略的名称，例如 `AMTRemote` 和对象标识符 `2.16.840.1.113741.1.2.1`。此策略允许导出用于服务器证书的私钥。

18 单击**确定**三次。添加应用程序策略之后，在 “应用程序策略描述” 列表中显示 “客户端验证” 策略和 `AMTRemote` 策略。

19 编辑 “颁发策略”，并单击**添加**。选择**全部颁发策略**选项，并单击**确定**两次。现在，“颁发策略描述” 列表中显示 “全部颁发策略” 选项。

20 在**安全**选项卡上，选择**域管理**，并且设置读、写、注册和自动注册权限。选择**企业管理**，并且设置读、写、注册和自动注册权限。选择**已验证用户**，并且设置读权限。

21 其他选项卡 （“颁发要求”、“取代的模板” 和 “主题名称”）不需要任何更改。

22 单击**应用**，然后单击**确定**。在 “证书模板” 的右窗格中显示 “客户端验证” 的新模板。

任务 4： 颁发客户端证书模板

在安装证书之前，必须颁发能够使模板成为证书的证书模板。

要颁发客户端证书模板，请执行以下步骤：

1 单击 Windows **开始**按钮，并选择**管理工具 > 证书颁发机构**。

2 展开安装的 Microsoft CA。右键单击 “证书模板”，并选择**新建 > 要颁发的证书模板**。此时将打开 “启用证书模板” 窗口。

3 选择在创建客户端证书模板 （第 17 页）中创建的客户端验证模板。在本示例中，它是 **ClientAuthTmpl** 模板。

4 单击**确定**。在 “证书模板” 窗口的右窗格中显示颁发的证书模板。

任务 5： 安装客户端证书

1 必须在安装 HPCA Server 的系统上以及 SCS Server 上安装客户端证书。

— 要在 SCS Server 或 HPCA Server 上安装客户端证书，请使用以下 URL：

`http://<FQDN_CAServer>/certsrv`

其中 *<FQDN_CAServer>* 是 Certification Authority Server 的完全限定域名。

可以在该计算机上从 Windows 桌面查找计算机的完全限定域名 (FQDN)。

a 右键单击**我的电脑**，选择**属性**。此时将打开 “系统属性” 窗口。

b 选择**计算机名**选项卡。此窗口中将显示计算机的 FQDN。

确保将此 URL 添加到浏览器的可信站点列表中。要添加此站点，请执行以下操作：

a 在浏览器中，转到**工具 > Internet 选项 > 安全**，并选择**可信站点**。

b 单击**站点**。此时将打开 “可信站点” 窗口。

c 在**将该网站添加到区域**中输入 URL。

d 清除**对该区域中的所有站点要求服务器验证 (https:)** 复选框。

e 单击**添加**。

f 单击**关闭**。

2 单击**请求证书 > 高级证书请求 > 创建请求并将请求提交给 CA**。

3 从**证书模板**下拉列表中选择客户端证书模板。在本例中，它是 `ClientAuthTmpl`。

4 在**标识脱机模板信息**中，**名称：**字段必须是将安装客户端证书的计算机的完全限定名称。

5 选中**将密钥标记为可导出**复选框。

6 单击**提交**。在随后的窗口中选择**是**，并安装证书。

任务 6： 导出客户端证书

*必须*为 HPCA Server 和 SCS Server 导出客户端证书。

要导出客户端证书，请执行以下步骤：

1 在服务器上，单击 Windows **开始**按钮，并选择**运行**。

2 输入 **MMC**，并单击**确定**。此时将打开 Microsoft Management Console。

3 从 “文件” 菜单中，选择**添加 / 删除管理单元**。

4 单击**添加**。

5 选择**证书**，并单击**添加**。

6 选择**我的用户帐户**，并单击**完成**。

7 单击**关闭**，然后单击**确定**。

8 从 Microsoft Management Console 的左面板中，展开 “证书 - 当前用户” 分支。

9 展开 “个人” 分支。

10 选择**证书**。

11 在右面板中，右键单击客户端证书。此时将打开一个弹出菜单。可以在**预期目的**选项卡上查找客户端证书。

12 选择**打开**。此时将打开 “证书信息” 窗口。

13 选择**详细信息**选项卡。

14 单击**复制到文件**。此时将打开 “证书导出向导” 的 “欢迎” 窗口。

15 单击**下一步**。此时将打开 “导出私钥” 窗口。

16 选择**是** > **导出私钥** > **下一步**。此时将打开 “导出文件格式” 窗口。单击**下一步**。

17 输入并确认保护私钥的密码。导入证书时，将需要此密码。单击**下一步**。

18 为要导出的文件输入完整的路径和名称。自动生成指示其文件类型 (`.pfx`) 的文件后缀。记下位置，因为将在后续步骤中需要访问它。

19 单击**下一步**，然后单击**完成**。

20 单击**确定**以关闭 “证书信息” 窗口。

任务 7： 导出根证书

在 vPro 设备和 HPCA Server 上都需要具有根证书，以验证服务器证书和客户端证书上的数字签名。

- 在 vPro 设备上， SCS Server 在配置设备的配置文件时使用根证书置备 vPro 设备。当 HPCA Server 向 vPro 设备发送其客户端证书时，在 vPro 设备上将使用根证书验证 HPCA Server 客户端的身份。
- 在 HPCA Server 上，根证书用于在 vPro 设备向 HPCA Server 发送其证书时验证设备的身份。根证书用于签署 vPro 设备以验证硬件和软件查询以及远程控制功能。

要将根证书导出到 Microsoft CA 服务器，请执行以下步骤：

1 单击 Windows **开始**按钮，并选择**管理工具** > **证书颁发机构**。此时将打开 “证书颁发机构管理控制台”。

2 在左窗口中，右键单击已安装的 Microsoft CA。从快捷菜单中，单击**属性**。此时将打开 “CA 属性” 窗口。

3 选择**常规**选项卡。

4 选择证书，并单击**查看证书**。

5 选择**详细信息**选项卡。

6 单击**复制到文件**。此时将打开 “证书导出向导”。

7 单击**下一步**。

8 选择 **DER encoded binary X.509 (.CER)** 作为导出文件格式 （默认选择）。

9 单击**下一步**。

10 为要导出的文件输入完整的路径和名称。自动生成指示其文件类型 (`.cer`) 的文件后缀。记下位置，因为将在后续步骤中需要访问它。

11 单击**下一步**，并查看设置。若要继续，请单击**完成**。此时将显示一条消息，指示导出成功。

12 单击**确定**。将返回到 “证书” 窗口上的**详细信息**选项卡。

13 单击**确定**以关闭 “证书” 窗口。

14 单击**确定**返回到 “证书颁发机构管理控制台”。关闭控制台。

15 将证书文件复制到 SCS Server 和 HPCA Server 上的位置。

任务 8： 将根证书转换成 PEM 格式

HPCA Server 上的根证书将转换成 PEM 格式，以便在开启 TLS 相互验证时，用于保护 IDE-R/SOL 操作。此转换在将根证书转换成 PEM 格式 （第 47 页）中进行了描述。

任务 9： 将客户端证书转换成 PEM 格式

客户端证书将安装到转换为 PEM 格式时所在的 HPCA Server 上，以便在开启 TLS 相互验证时，用于保护 IDE-R/SOL 操作。此转换在将客户端证书转换成 PEM 格式（第 47 页）中进行了描述。

任务 10：将根证书导入到 JRE

在 HPCA Server 上，根证书将添加到 Java 密钥库中，以便在设备向 HPCA Server 发送其服务器证书时验证 vPro 设备服务器的身份。此转换在将根证书导入 Java 密钥库 （第 46 页）中进行了描述。

任务 11：配置安全参数

必须指定 PEM 和 PFX 客户端证书的密码，并为 TLS 验证设置配置参数，如配置安全参数（第 35 页）中所述。

任务 12：重新启动 Tomcat 服务

重新启动 **HPCA Tomcat Server** 服务。

设置 SCS Server

必须配置 “设置与配置服务” 以保证与 vPro 设备的所有通信的安全。在 SCS Server 上安装此软件。

安装 “设置与配置服务”

要安装 “设置与配置服务” 的组件，请参见 《Intel 设置与配置服务安装指南 V5.4》 (Intel Setup and Configuration Service Installation Guide Version 5.4) 中的 “安装 (Installation)” 一章。

登录到 SCS Console

登录到 SCS Console：

1 在 SCS Server 上，单击 Windows **开始**按钮，并选择 **Intel AMT 配置** → **Intel AMT SCS Console**。此时将打开登录窗口。

2 在 “服务名称” 字段中，输入 SCS Web 服务的 URL 路径 （包括虚拟目录）。格式为 **<**`http|https`**>://**`<FQDN of Provision Server>/<SCS Web 服务的虚拟目录>`。

   此时将打开 “SCS Console”。

配置 SCS 服务设置

在 “SCS 服务设置” 窗口中，必须为 Active Directory Integration 选择**无**。

有关如何配置 SCS 服务设置的详细信息，请参见 《Intel 设置与配置服务控制台用户指南 V5.4》 (Intel Setup and Configuration Service Console User Guide Version 5.4) 中的 “查看并配置 SCS 服务 (Viewing and Configuring SCS Services)” 一章。

创建和配置配置文件

此配置文件与 vPro 设备关联，如添加新 vPro 系统 （第 24 页）中所述。配置文件在置备过程期间向 vPro 设备提供初始值。

配置配置文件：

在 “可选设置” 窗口中，启用以下选项：

— **ACL**

— **对平台上的操作使用 TLS 安全通信** （仅在计划使用 TLS 通信时需要。）

— **允许连接到 WiFi 网络** （仅在要使用无线 NIC 进行管理时需要。）

在 “ACL 详细信息” 窗口中，指定以下内容：

— 用户类型：选择 **Digest 用户**。

— 用户 / 组名称：输入此帐户类型的用户名。

— 密码：输入帐户的密码，并启用**掩码**。

— 访问类型：从列表中选择**两者**。

— 领域：在列表中选择适当的领域。使用 HPCA Console 管理 vPro 设备时，领域确定用户帐户可以执行的操作的类型。建议为创建的第一个帐户选择所有领域（安全审核日志领域除外）。

在 TLS 窗口中，指定以下内容（仅在计划使用 TLS 通信时需要执行此操作）：

— 在基本 TLS 配置下：对于 TLS Server 证书颁发机构，从列表中选择一个**证书颁发机构**。对于服务器证书模板，从列表中选择 **WebServer**。

— 在高级 TLS 配置下：选中**使用相互验证**复选框。在列表中选择所需的 TLS 可信根证书。

— 单击**添加**。此时将打开“添加可信根证书”窗口。在此窗口中，选中**从文件**单选按钮，并浏览到导出的根证书。可以查看证书。单击**确定**以完成任务。

如果计划通过路由器的无线访问点配置 WPA-TKIP 配置文件，必须在“WiFi 配置文件”窗口中进行以下选择：

— 配置文件名称：输入配置文件的唯一名称（例如， PSGWirelessProfile）以区别于常规配置文件名称。

— SSID：输入在路由器无线访问点中设置 WPA-TKIP 配置文件时使用的 SSID 值。请参见无线路由器文档。

— 密钥管理协议：从列表中选择 **WiFi 保护的访问 (WPA)**。

— 加密算法：从列表中选择**临时密钥完整性协议 (TKIP)**。

— 通行密码：选中**通行密码**单选按钮。输入在路由器无线访问点中设置 WPA-TKIP 配置文件时使用的通行密码值。请参见无线路由器文档。

➤ 如果要配置具有无线接口的 vPro 设备的配置文件，则必须首先在无线路由器的无线访问点中配置 WPA-TKIP 配置文件。需要参见无线路由器附带的文档。

有关如何创建和配置配置文件的详细信息，请参见《Intel 设置与配置服务控制台用户指南 V5.4》(Intel Setup and Configuration Service Console User Guide Version 5.4) 中的“创建和更改配置文件 (Creating and Changing Profiles)”一章。

置备 vPro 设备

默认情况下， Intel vPro 设备以未配置状态（工厂模式）交付。在管理应用程序可以访问 vPro 设备之前，设备必须填充配置设置，包括安全通信所需的用户名、密码、网络参数、 TLS 证书和 PID-PPS 密钥。

通过输入每台设备的管理引擎 BIOS 扩展 (MEBx) 和手动输入所需信息，可以配置 vPro 设备。手动置备设备使用预共享密钥 (PSK) 模式来保护 SCS Server 和 vPro 设备之间的通信。有关详细信息，请参见使用 MEBx 配置 vPro 设备（第 24 页）。

或者，也可以通过利用自动置备设备的 Intel 远程配置过程来配置设备。置备设备自动使用公钥基础结构 (PKI) 保护通信。有关详细信息，请参见使用远程配置配置 vPro 设备（第 24 页）。

使用 MEBx 配置 vPro 设备

任务 1： 配置安全密钥

有关如何配置安全密钥的信息，请参见 《Intel 设置与配置服务控制台用户指南 V5.4》 (Intel Setup and Configuration Service Console User Guide Version 5.4) 中的 “对 TLS-PSK 密钥使用 USB 驱动器 (Using USB Drives for TLS-PSK Keys)” 一章下的 “配置预设置和配置安全密钥 (Configuring Pre-Setup and Configuration Security Keys)” 一节。

➤ 建议在 “创建 TLS-PSK 密钥” 窗口中选择**固定密码**，并提供新密码。

任务 2： 通过 MEBx 配置 vPro 设备。

请参见设备供应商文档以了解确切步骤。必须设置以下参数，才能通过 MEBx 配置 vPro 设备：

— 输入 vPro 设备的主机名。

— 启用 TCP/IP。

— 启用 DHCP。

— 选择 **Provisioning Server**。输入要用于运行 Intel SCS 的计算机的 IP 地址。

— 将监听端口设置为 9971。

— 将 PID 和 PPS 设置为在配置安全密钥时指定的值。

任务 3： 添加新 vPro 系统

有关添加新 vPro 系统的信息，请参见 《Intel 设置与配置服务控制台用户指南 V5.4》 (Intel Setup and Configuration Service Console User Guide Version 5.4) 中的 “准备和管理平台 (Preparing and Managing Platforms)” 一章下的 “添加平台定义 (Adding a Platform Definition)” 一节。

使用远程配置配置 vPro 设备

远程配置是启用设置时无需在每台设备上手动安装 PID/PPS 对的 vPro 机制。要利用远程配置，必须执行以下操作：

任务 1： 从可信证书颁发机构 (CA) 购买安全证书。

CA 供应商必须是根证书哈希值内置到 vPro 固件中的供应商之一。转到选择的供应商网站以购买 SSL 证书。每个站点说明了请求、注册、安装和移动 SSL 证书所需的步骤。必须在安装 SCS Server 的系统上安装系统证书存储中的证书。有关详细信息，请参见 《Intel 设置与配置服务控制台用户指南 V5.4》 (Intel Setup and Configuration Service Console User Guide Version 5.4) 中的 “远程配置 (Remote Configuration)” 附录中的 “远程配置流程 (Remote Configuration Flow)” 一节。

任务 2： 远程配置 vPro 设备

通过远程配置置备 vPro 设备有两种方式。它们分别是：

- vPro 设备的裸机远程配置，如 vPro 设备的裸机远程配置 （第 25 页）中所述。
- 通过 OOBM 代理程序进行的延迟远程配置置备，如 vPro 设备的延迟远程配置置备（第 25 页）中所述。

vPro 设备的裸机远程配置

通常，在将 vPro 设备连接到网络时立即设置 vPro 设备 （如果已经正确执行远程配置要求）。这称为*裸机配置*。设备将开始把 “Hello” 消息发送到 SCS Server，以指示它已经转换成设置模式。如果设备可以在为其打开网络接口的有限网络访问时间间隔内成功置备，则无需执行进一步的置备任务。

对于 HP 台式机，有限网络访问时间间隔是 255 小时。在时间间隔结束之后，如果没有通过来自 SCS 的网络命令延长设置与配置时间，则接口将关闭。

执行 vPro 设备的裸机配置

1. 将 vPro 设备连接到 SCS Server 所在的网络。 vPro 设备必须连接到已安装 SCS 的相同域中。
2. 打开 vPro 设备。

   vPro 设备将自动发送 “Hello” 数据包。在 vPro 设备从 SCS Server 接收消息之后，启动置备过程，在此过程中 SCS Server 加载启用 vPro 设备所需的所有设置和数据。
3. 在配置 vPro 设备之后，安装操作系统。可以从网络将特定于 IT 的操作系统安装到允许 vPro 系统的完全 “无键” 配置的 vPro 设备上。

裸机远程配置失败

尽管 vPro 设备连通网络和交流电源后即刻启动裸机置备过程，但该设备可能无法在其有限网络访问时间段内成功置备。失败的原因包括：

- OTP 已在 SCS Server 上启用
- 网络流量过多
- 证书与 vPro 设备上的根哈希值不匹配

vPro 设备的延迟远程配置置备

如果裸机配置失败，则可以通过使用延迟远程配置来置备设备。要了解转换为设置模式期间以及延迟远程配置置备过程中发生的情况，请参见附录 B， vPro 设备的延迟远程配置。

建议在工作流程中的这一时间点安装 OOBM 代理程序。如果 vPro 设备在裸机配置的有限时间段内无法成功置备，则 OOBM 代理程序将在未置备设备上调用延迟配置，作为其安装过程的一部分。

安装 OOBM 代理程序

可以使用两种方式在 vPro 设备上安装 OOBM 代理程序。一个方式是在每个 vPro 设备上手动安装 OOBM 代理程序。另外，也可以通过 HP Client Automation Standard 或 Enterprise 软件将 OOBM 代理程序自动安装到多个 vPro 设备上。

在以下各节中描述这两种方法。

配置客户端角色

要通过 OOBM 代理程序置备 vPro 设备，不管选择哪种安装方法，都必须执行以下操作：

- 必须在 SCS Console 中创建和添加具有配置客户端角色的用户。例如，在 SCS Console 中创建和添加的用户可以命名为 **SCSUser**。
- 此用户必须在域 **VLAN1** 中创建，例如， **SCSUser@vlan1.hp.com**。

需要在 OOBM 代理程序安装期间提供具有配置客户端角色的用户的凭据。必须正确提供 SCS 配置客户端的用户凭据，否则 OOBM 代理程序将无法通过延迟设置启动设备的置备。

在安装 OOBM 代理程序时，必须提供 “虚设” 用户名和密码，即使不打算使用延迟配置来置备设备也是如此。如果不提供用户名和密码，安装将失败，返回错误代码 1920。

在某些情况下，要查看 OOBM 代理程序安装或者服务重新启动的结果，可以在事件日志中查看错误代码为 1063 的错误消息。此错误无害，可以忽略。

在单个 vPro 设备上手动安装 OOBM 代理程序

在 vPro 设备上手动安装 OOBM 代理程序

1. 将位于 HPCA Core 分发介质 `\Media\client\default\win32\oobm\LocalAgent` 目录下的 `oobmclocalagent.msi` 文件复制到 vPro 设备。双击 `oobmclocalagent.msi` 文件。或者，您还可以将位于分发介质上同一目录下的 `setup.cmd` 文件复制到 vPro 设备。双击 `setup.cmd` 文件，或在命令行中输入 `setup.cmd`。 `setup.cmd` 文件会调用 `oobmclocalagent.msi` 文件。
2. 单击**下一步**，并接受许可协议。
3. 单击**下一步**。此时将打开 “远程配置参数” 窗口。在此窗口中，指定以下信息：
   - SCS 配置客户端用户名：输入具有配置客户端角色的用户的名称。格式为 *SCS_User_Name@Domain_Name*。
   - SCS 配置客户端密码：输入具有配置客户端角色的用户的密码。
   - SCS 配置文件标识：输入 vPro 设备的配置文件标识。此信息可以在 SCS Console 的 “配置文件” 区域中找到。
   - SCS 远程配置 URL：输入包括 Intel 设置与配置服务 (SCS) 远程配置服务的虚拟目录的 URL 路径。例如 **https://provisionserver.yourenterprise.com/amtscs_rcfg**，其中 **provisionserver.yourenterprise.com** 是 IIS 主机的完全限定域名 (FQDN)，**amtscs_rcfg** 是主机上的 SCS 远程配置服务虚拟目录。

4 单击**下一步**。此时将打开 “用户信息” 窗口，该窗口允许为上一步骤中引用的 SCS 配置文件标识中定义的用户输入 vPro Digest 用户凭据。在此窗口中，指定以下信息：

— 用户名：输入在 SCS 配置文件中定义的 Digest 用户的 vPro 用户名。

— 密码：输入在 SCS 配置文件中定义的 Digest 用户的 vPro 密码。

— 如果在 TLS 模式下置备 vPro 设备，则选中 **TLS 模式**复选框。

5 单击**下一步**，然后执行安装向导中的其余步骤。

OOBM 代理程序是 NT 服务，安装后立即启动。

通过 Client Automation 在多个 vPro 设备上自动安装

如上所示，可以通过 HP Client Automation Standard 或 Enterprise 软件在多个设备上自动安装 OOBM 代理程序。

如果使用的是 HP Client Automation 软件的 Starter 版本，则无法使用此方法安装 OOBM 代理程序。

自动安装过程包括两个部分。它们分别是：

- 必须通过使用 HP Client Automation Administrator Publisher，将 OOBM 代理程序软件发布到 HP Client Automation Configuration Server 数据库。
- 必须通过使用 HPCA Console，将 OOBM 代理程序部署到 vPro 目标设备。

将 OOBM 代理程序发布到 Client Automation 数据库

1 单击**开始** > **程序** > **HP Client Automation Administrator** > **Client Automation Administrator Publisher** 以调用 HP Client Automation Administrator Publisher。此时将打开 “登录” 窗口。

2 使用 HP Client Automation 用户名和密码登录到 HP Client Automation Administrator Publisher。默认情况下，用户名是 `admin`，密码是 `secret`。此时将打开 “发布选项” 对话框窗口。

3 从列表中选择 **Windows Installer**。

4 单击**确定**。将打开 “选择” 向导。

5 在左导航菜单中选择 OOBM 代理程序安装程序文件 (`oobmclocalagent.msi`) 作为要发布的 Windows Installer 文件。

6 单击**下一步**。将打开 “编辑” 向导。

7 单击**属性**链接。安装程序文件的属性将显示在右侧。确保正确设置了从 **AMT** 开始的所有属性。这些属性包括：

— AMTUSERNAME：输入 vPro 管理员的用户名 （Digest 用户名）。

— AMTPASSWORD：输入 vPro 管理员的密码 （Digest 用户密码）。

— AMTTLSMODE：如果在 TLS 模式下置备 vPro 设备，输入 **1**，否则，输入 **0**。

— AMTPROVSERVERADD：输入包括 Intel 设置与配置服务 (SCS) 远程配置服务的虚拟目录的 URL 路径。

— AMTPROFILEID：输入 vPro 设备的配置文件标识。此信息可以在 SCS Console 的 “配置文件” 区域中找到。

8 还要确保在属性页上正确设置了以下属性：

— SCSUSERNAME：输入具有配置客户端角色的用户的名称。

— SCSUSERPASS：输入具有配置客户端角色的用户的密码。

9 单击**下一步**。将打开 “配置” 向导。

10 在 “配置” 窗口中，指定以下信息 （未列出的字段是可选字段）：

— 服务标识：输入文本字符串以标识服务，例如， **HP_CA_OOB_LOCAL_AGENT**。

— 描述：输入软件的描述，例如， **HP CA OOB Local Agent**。

— 软件目录：从列表选择**用户应用程序**。

— 程序包限于以下系统：如果不选择任何操作系统，则不管操作系统如何，软件将部署到所有 vPro 设备。

➤ 字段可能会因 HPCA 许可证的不同而不同。

11 单击**下一步**。将打开 “发布” 向导。显示 “摘要” 和 “进度” 信息。

12 单击**发布**。 OOBM 代理程序应用程序将发布到 HP Client Automation Configuration Server 数据库。

13 单击**完成**。

14 在弹出窗口中单击**是**以退出 HP Client Automation Administrator Publisher。

将 OOBM 代理程序自动部署到多个 vPro 设备

有关以下过程的详细说明，请参见 Standard 或 Enterprise 版的《HP Client Automation Core 和 Satellite 用户指南》 (HP Client Automation Core and Satellite User Guide)。

1 将 vPro 设备导入到 HPCA 中。

2 将 OOBM 代理程序部署到目标 vPro 设备。

3 创建静态组，并将目标 vPro 设备添加到该组。

4 将 OOBM 代理程序部署到 vPro 设备组。

检查 vPro 设备上 OOBM 代理程序的版本

检查 OOBM 代理程序的版本

1 转到 vPro 设备上的安装目录 < *安装目录* >\`OOBM Agent`。

2 右键单击 `OOBMCLocalAgent.exe` 文件，并从上下文菜单选择**属性**。

3 选择**版本**选项卡。在此窗口中显示版本信息。

64 位平台上的 OOBM 代理程序

如果在 64 位平台上安装 OOBM 代理程序，则必须确保在 vPro 设备上安装了 32 位和 64 位平台的特定于 Intel 的驱动程序。可以在 **http://www8.hp.com/cn/zh/support-drivers.html** 处找到这些驱动程序。对于台式机，可以在 “软件 – 系统管理” 部分下找到驱动程序。驱动程序的名称是 Intel 本地管理服务 (LMS) 和 Serial-over-LAN (SOL) 支持。对于笔记本电脑，驱动程序通常位于 Windows 安装目录的 `SWSetup\AppInst` 目录下。如果不是，则还可以从上面提到的 HP 支持站点下载这些驱动程序。在驱动程序安装之后，必须重新启动系统。

查看 vPro 设备

在置备 vPro 设备之后，可以在 vPro SCS Console 中查看它。

➤ 可能必须等待一点时间才能在控制台中看到设备。

查看 vPro 设备

1 打开 vPro SCS Console。

2 展开 “平台收集” 分支。

3 双击**所有平台**查看 vPro 设备。显示 vPro 设备置备状态。

更改验证模式

➤ 仅当设置了 TLS 验证时，这一节才相关。如果尚未设置 TLS，则跳到 OOBM 配置章。

在置备 vPro 设备之后，可以通过使用 vPro SCS Console 更改设备的验证模式。

将 vPro 设备配置为 TLS 服务器验证模式

1 打开 vPro SCS Console。

2 展开配置服务设置分支，并选择**配置文件**。它列出了为不同 vPro 设备创建的配置文件。

3 选择 vPro 设备的适当配置文件，并单击**编辑**。

4 选择**网络**选项卡，并选择以下选项：

— 使用 TLS

— 用于本地和远程接口的 TLS 服务器验证

5 单击**应用**，然后单击**确定**。返回到主 SCS Console。

6 展开 Intel AMT 系统分支，并选择**全局操作**。此时将打开 “全局操作” 窗口。

7 在此窗口的 “置备” 窗格中，单击**重新置备**。它会将一个请求标识分配给此重新置备请求。记下此标识，因为在 “操作状态” 日志中搜索日志信息时可以使用它。

8 单击**确定**。

9 展开日志分支，并选择**操作状态**。此日志显示所有请求的状态。可以通过使用在上一步骤中分配的请求标识，检查重新置备请求是否成功。

将 vPro 设备配置为 TCP 模式

1 打开 vPro SCS Console。

2 展开配置服务设置分支，并选择**配置文件**。它列出了为不同 vPro 设备创建的配置文件。

3 选择 vPro 设备的适当配置文件，并单击**编辑**。

4 选择**网络**选项卡，并清除**使用 TLS** 复选框。

5 单击**应用**，然后单击**确定**。返回到主 SCS Console。

6 展开 Intel AMT 系统分支，并选择**全局操作**。此时将打开 “全局操作” 窗口。

7 在此窗口的 “置备” 窗格中，单击**重新置备**。它会将一个请求标识分配给此重新置备请求。记下此标识，因为在 “操作状态” 日志中搜索日志信息时可以使用它。

8 单击**确定**。

9 展开日志分支，并选择**操作状态**。此日志显示所有请求的状态。可以通过使用在上一步骤中分配的请求标识，检查重新置备请求是否成功。

设置 DASH 设备

DASH 配置

按照设备随附的文档置备已启用 DASH 的设备。

对于来自 Hewlett-Packard 的已启用 DASH 的设备， DASH 配置信息记录在 《Broadcom NetXtreme Gigabit Ethernet Plus NIC》白皮书中。

访问此文档

1 转到 **http://www8.hp.com/cn/zh/home.html**。

2 选择**支持与驱动程序 > 产品使用和问题解决**。

3 输入支持此网卡的产品 （例如， dc7900）。

4 选择 dc7900 的一个型号。

5 选择**手册 （指南、补遗和附录等）**。

6 滚动到白皮书部分，并选择 **Broadcom NetXtreme Gigabit Ethernet Plus NIC** 白皮书。

DASH 配置实用程序

DASH 配置实用程序 （BMCC 应用程序）是 Broadcom NetXtreme Gigabit Ethernet Plus NIC 驱动程序 softpaq 的一部分，可以在每个支持此网卡的产品的驱动程序部分中找到。

访问此实用程序

1 转到 **http://www8.hp.com/cn/zh/home.html**。

2 选择**支持与驱动程序 > 驱动程序和软件下载**。

3 输入支持此网卡的产品 （例如， dc7900）。

4 选择 dc7900 的一个型号。

5 选择操作系统。

6 滚动到 “驱动程序更新 - 网卡”部分，并选择下载 **Broadcom NetXtreme Gigabit Ethernet Plus NIC 驱动程序**。

3 OOBM 配置

本章解释了通过 HPCA 安装程序安装带外管理 (OOBM) 之后如何对其进行配置。有关系统要求和安装方面的信息，请参见位于以下网址的 《HP Client Automation Enterprise Edition 入门和概述指南》(HP Client Automation Enterprise Edition Getting Started and Concepts Guide) 以及《HP Client Automation 8.10 支持列表》 (HP Client Automation 8.10 Support Matrix)：**http://h20230.www2.hp.com/sc/support_matrices.jsp**。

在本章中介绍的配置任务为可选任务。如果要更改 OOBM 的默认设置，则可以执行这些任务。

配置参数信息

重新配置 SCS 路径

如有必要，可以更改当前通过 HPCA Console 配置的 SCS 路径。有关详细信息，请参见设置配置参数 （第 36 页）。

重新配置 Client Automation Web 服务

必要时，可以更改 HPCA Console 的网关 URL。比如， URL 是 `http://CAhost:3466/ca`，其中 *CAhost* 是 Client Automation 服务器的完全限定名称，*ca* 是 Client Automation 服务器上的 Client Automation Web 服务虚拟目录。有关详细信息，请参见设置配置参数 （第 36 页）。

配置 IDE-R 驱动器

当使用电子集成驱动器重定向 (IDE-R) 时，按 CD 和软盘驱动器的默认设置在服务器上安装 OOBM 软件。这些设置是可配置的。有关详细信息，请参见设置配置参数 （第 36 页）。如果默认设置与服务器上的驱动器规范不一致，则必须更改默认驱动器设置以与服务器相符。 CD 和软盘驱动器路径必须指向真实的驱动器或映像。

➤ 即便使用 “软盘驱动器”引导选项时， CD/DVD 配置也必须设置正确 （即，指向真实的 CD/DVD 驱动器）。使用 “CD/DVD 驱动器”引导选项时，软盘配置亦是如此。如果 HPCA 服务器中未连接软盘驱动器，则可以指向任何可引导的本地 ISO 映像 （而非软盘驱动器）以进行 IDE-R 操作。

➤ 如果分别修改 CD 或软盘驱动器设置以使用 ISO 或 IMG 文件（相对于物理 CD 或软盘），则运行 Tomcat 的服务器必须能够看到 ISO 或 IMG 文件的驱动器路径。因此，要将所有必需的 ISO 和 IMG 文件复制到运行 Tomcat 的服务器的本地驱动器中。

而且，如果 ISO 或 IMG 文件是共享网络资源，则必须使用通用命名约定 (UNC) 语法才能访问网络文件。 UNC 语法如下：*hostname**sharefolder**file*

采用 UNC 语法时，必须使用计算机的真实主机名，而不是其 IP 地址。

配置 SOL 端口

在 HPCA 服务器上安装 OOBM 软件使用的是 serial over LAN (SOL) 启动端口和一次可打开的最大 SOL 端口数的默认设置，以便 vPro 设备上同时有多个 SOL 会话打开。这些值可以更改。有关详细信息，请参见设置配置参数 （第 36 页）。

➤ 在 vPro 设备上， SOL 会话启动 Windows HyperTerminal，后者与大多数 Windows 操作系统绑定。请检查用于访问 HPCA Server 的 Web 浏览器计算机上是否已安装 HyperTerminal。如果尚未安装 HyperTerminal，请参见 Microsoft 文档以获取安装说明。

HyperTerminal 不与 Windows Vista 操作系统捆绑。在这种情况下， SOL 会话启动 Telnet。

配置 SNMP 端口

这是用于从 vPro 设备获取警告消息的 SNMP 端口。此端口是可配置的。有关详细信息，请参见设置配置参数 （第 36 页）。

配置 IDE-R 和 SOL 超时值

在 vPro 设备上通过无线网络接口卡执行的远程操作可由于超过 IDE-R 和 SOL 会话的超时值而失败，因为无线通信的速度一般较慢。 IDE-R 和 SOL 超时与检测信号间隔值是可配置的。有关详细信息，请参见设置配置参数 （第 36 页）。

配置 Web 服务超时值

OOBM 服务通过向设备发出 Web 服务调用与 vPro 设备进行通信。已为此通信指定超时值。如果此值不适合于当前网络状况，则可以重新配置。有关详细信息，请参见设置配置参数（第 36 页）。

配置 DASH 设备的缓存大小

您可以为特定用户会话配置内存中要缓存的 DASH 设备数。有关详细信息，请参见设置配置参数 （第 36 页）。修改此值会影响性能。此值取决于内存资源的可用性。

配置安全参数

➤ 只有在配置了 TLS 后才需要执行此步骤。

➤ 如果启用了 TLS AMT 验证，则 Tomcat 服务器必须在域用户帐户下运行，才具有访问 Java 密钥库的适当权限。

对于 TLS 验证，必须设置许多配置参数。 OOBM 利用这些参数可以定位可信的根和客户端证书，以获悉与之关联的密码和证书授权机构服务器的 FQDN。

您必须配置以下参数：

- PEM 格式的根证书完整路径名 (`root_certificate`)
- PEM 格式的客户端证书完整路径名 (`client_certificate_pem`)
- PFX 格式的客户端证书完整路径名 (`client_certificate_pfx`)
- 客户端证书 CN (`ca_server_commonname`)

有关如何设置以上参数的信息，请参见设置配置参数 （第 36 页）。

有关 PEM 格式的证书的信息，请参见将证书转换成 PEM 格式 （第 47 页）。

此外，必须指定 PEM 和 PFX 客户端证书的密码。在以下过程中执行命令时，请指定无双引号的路径。

指定 PEM 客户端证书密码

1 在 <*安装目录*>/OOBM/bin 目录下，运行 `amtpem_chgpwd.bat` 文件。

2 在出现提示时，输入 HPCA 安装目录。

3 在出现提示时，输入 PEM 客户端证书的密码。

指定 PFX 客户端证书密码

1 在 <*安装目录*>/OOBM/bin 目录下，运行 `amtpfx_chgpwd.bat` 文件。

2 在出现提示时，输入 HPCA 安装目录。

3 在出现提示时，输入 PFX 客户端证书的密码。

配置监视程序设置

创建监视程序时，适用于监视程序的两个设置是：OOBM 代理程序的检测时间间隔 （两次将检测信号发送到监视程序之间的时间间隔），和 OOBM 代理程序开始将检测信号发送到监视程序之前的启动时间。您可以更改默认值以反映网络需要。有关详细信息，请参见设置配置参数（第 36 页）。

用于调试的配置设置

有两个配置参数可用来帮助调试与性能相关的问题。它们是 `cache_update_thread_size` 和 `blocking_timer_time` 参数。

`cache_update_thread_size` 参数允许您更改用于更新缓存层的线程数。正常情况下，不需要更改此值。但是，在结合 `blocking_timer_time` 参数时可更改此值，以解决性能问题。

如果在调用 vPro Web 服务时 HPCA 服务器上出现任何套接字问题，则可以使用 `blocking_timer_time` 设置更改超时值。如果存在任何与套接字相关的问题，建议增加超时值。

有关详细信息，请参见设置配置参数 （第 36 页）。

设置配置参数

您可以通过修改 `<HPCA_Install_DIR>\oobm\conf\` 目录下的两个属性文件来设置配置参数。

如果更改此目录下属性文件的配置参数，则必须重新启动 Tomcat 服务

在 `config.properties` 文件中可以找到或添加以下参数。您可以编辑此文件以重新配置下列任意参数的值，方法是为现有的**键 = 值**对输入新值或添加新的**键 = 值**对。

在 `config.properties` 中指定路径和完全限定文件名时，必须使用 “`\\`” 或 “`/`” 作为目录分隔符，否则无法正确读取文件名。例如， `C:\\certs\\cc.pem` 或 `C:/certs/cc.pem` 是正确的，而 `C:\certs\cc.pem` 是错误的。

下表列出了此文件中包含的参数及其默认设置和描述。

表 4　config.properties 文件中的配置参数

参数 （键）	默认值	描述
scsserver_url	无默认值	SCS Server 的 URL。可以更改当前配置的 SCS 路径。
radia_gateway	无默认值	HPCA Console 的 URL

表 4　**config.properties** 文件中的配置参数 （续）

参数 （键）	默认值	描述
default_cddrive_path	D:	默认的 IDE-R CD 驱动器设置。CD 路径必须指向真实驱动器或映像。
default_fddrive_path	A:	默认的 IDE-R 软盘驱动器设置。软盘驱动器路径必须指向真实驱动器或映像。
sol_port_start	9999	启动 SOL 端口
sol_number_of_port	10	最大 SOL 端口数
snmp_trapd_port	162	SNMP 端口
vPro_webservice_timeout	15000 毫秒	Web 服务超时值
devices_cachequeuesize	50	DASH 设备的缓存大小。修改此值会影响性能。
root_certificate	无默认值	PEM 格式的根证书完整路径名
client_certificate_pem format	无默认值	PEM 格式的客户端证书完整路径名
client_certificate_pfx	无默认值	PFX 格式的客户端证书完整路径名
ca_server_commonname	无默认值	客户端证书 CN
apwatchdog_heartbeat_interval	60 秒	监视程序 OOBM 代理程序检测信号间隔
apwatchdog_startup_time	300 秒	监视程序 OOBM 代理程序启动时间间隔
device_synchronization_timeperiod	0	从 SCS 储备库重新加载设备列表的时间段。同步时间间隔的默认值为零，表示不会自动同步。如果希望自动同步，请将其设为非零值。此值的单位是分钟。

表 4　**config.properties** 文件中的配置参数 （续）

参数 （键）	默认值	描述
group_synchronization_timeperiod	0	从 CA 储备库重新加载组设备的时间段。同步时间间隔的默认值为零，表示不会自动同步。如果希望自动同步，请将其设为非零值。此值的单位是分钟。
cache_update_thread_size	25	缓存线程大小 （仅用于调试）
blocking_timer_time	100	阻止超时值 （仅用于调试）
devices_cachequeuesize	100	用于存储与 vPro 相关的 Java 对象的缓存大小，这些对象用于执行诸如电源管理、系统防御功能部署等操作（仅限于调试目的）。
scsserver_url	无默认值	SCS Server 的 URL。可以更改当前配置的 SCS 路径。
radia_gateway	无默认值	HPCA Console 的 URL

在同样位于 `<`*HPCA 安装目录*`>\oobm\conf\` 目录的 `configuration.properties` 文件中可以找到其他配置参数。已为所有这些参数分配了默认值，但某些参数可能需要重新配置，具体取决于安装。表 5 列出了此文件中包含的参数及其默认设置和描述。

此文件中的数据对带外管理的正确运行而言至关重要。确保不修改或删除表 5 **描述**列中列为“最终用户不适用”的项。

表 5　**configuration.properties** 文件中的配置参数

参数	默认值	描述
Active_Directory_FQDN_or_Hostname_property	name	从 AD 返回的设备标识信息。您可以选择主机名 (**name**) 或 FQDN (**dNSHostName**)。使用默认值 (name) 较为安全，因为 FQDN 可能会由于子域 DNS 而失败。
BEV_BOOT_SOURCE_VALUES	BEV	引导条目矢量的引导源名称
CACHE_SIZE	50	OOBM Web 服务系统的缓存大小。例如，`CACHE_SIZE=50` 指定系统任何时候最多只能缓存 50 台设备。当缓存已满且需要添加新设备时，删除最少访问/使用的设备以容纳新设备。
CACHE_WAIT_DURATION	2000	缓存等待持续时间 （以毫秒为单位）。例如，`CACHE_WAIT_DURATION=2000` 指定系统等待缓存管理器响应的时间不应超过 2000 毫秒。如果缓存管理器在 2000 毫秒以后仍忙碌，系统不会在当前操作中使用缓存。
CDDVD_BOOT_SOURCE_VALUES	CD/DVD，CD-ROM	CD 的引导源名称
DASH_PORTS	623	DASH 端口的逗号分隔列表
DASH_TEXTREDIRECTION_TIME_DELAY	2	文本重定向连接和电源操作调用之间的时间延迟 （以秒为单位）。
DISCOVERY_DELAY	100	发现延迟时间。增加此值可解决套接字连接耗尽的问题。

表 5　**configuration.properties** 文件中的配置参数 （续）

参数	默认值	描述
DISCOVERY_REQUEST	包含 DASH 发现请求的实际内容	DASH 设备发现的 DASH 请求内容。
DISCOVERY_SEQUENCE	dash,vpro	发现 OOBM 设备的顺序。例如，`DISCOVERY_SEQUENCE ="dash,vpro"` 表示系统先检查设备是否为 DASH 设备，如果不是，再检查是否为 vPro 设备。
ENABLE_BLIND_DISCOVERY	true	OOBM 设备的盲发现。如果启用，系统将允许对当前未发现的 OOBM 设备的操作请求，方法是先自动发现这些设备，然后执行请求的操作。如果禁用，则 OOBM 系统中应当已经发现 OOBM 设备。否则，系统将会出错。
FLOPPY_BOOT_SOURCE_VALUES	Floppy，Diskette Drive	软盘的引导源名称
HDD_BOOT_SOURCE_VALUES	Hard Drive,Hard-Disk	硬盘驱动器的引导源名称
HTTP_CONNECT_TIMEOUT	3000	HTTP 连接超时 （HTTP 连接等待响应的最大毫秒数）
HTTP_READ_TIMEOUT	200	HTTP 读取时间 （HTTP 连接等待读取响应的最大毫秒数）

表 5　**configuration.properties** 文件中的配置参数 （续）

参数	默认值	描述
IDER_CLIENT_RX_TIMEOUT	10000	客户端接收超时值（以毫秒为单位）。如果超时值已到，而客户端还没有从 HPCA Server 接收到任何消息，客户端将关闭 IDE-R 会话。当 IDE-R 会话打开时， HPCA Server 将继续发出消息，以确保客户端接收超时值不会逾期（HPCA Server 检测信号间隔基于客户端接收超时的设置）。 最小值：10000 最大值：65535 默认值：10000
IDER_CLIENT_COMMAND_TIMEOUT	0	客户端命令传输超时值（以毫秒为单位）。这是客户端在发出 IDE 命令时等待的时间值。如果客户端没有在指定的时间内从 HPCA Server 接收到命令响应，则将关闭 IDE-R 会话。值 0 表示不使用命令传输超时。 最小值：0 最大值：65535 默认值：0
IDER_CLIENT_HB_INTERVAL	5000	客户端检测信号间隔 （以毫秒为单位）。这是客户端在将检测信号消息发送到 HPCA Server 前等待的时间值。值 0 表示不发送检测信号消息。在这种情况下，如果没有任何活动可以确定 IDE-R 是否仍在运行，HPCA Server 将定期向客户端发送保持 IDE-R 活动的 Ping 消息。 最小值：0 最大值：65535 默认值：5000

表 5　**configuration.properties** 文件中的配置参数 （续）

参数	默认值	描述
NETWORK_BOOT_SOURCE_VALUES	Network,PXE	PXE 的引导源名称
NUMBER_OF_DISCOVER_WORKER_THREADS	5	可用于发现的最大线程数
PCMCIA_BOOT_SOURCE_VALUES	PCMCIA	PCMCIA 的引导源名称 （更多信息请访问：http://zh.wikipedia.org/wiki/PC_card）
REVERTBACK_PREVIOUS_BOOT_ORDER	0	引导顺序重置标志。在用特定引导源引导设备时，可以选择禁用 (**0**) 或启用 (**1**)，以返回引导配置的上一个引导顺序。默认设置是禁用返回，否则会影响性能。
RevertBack_Previous_Boot_Order_Wait_Timer	10000	初始化重新启动操作后，等待返回上一个引导顺序的时间 （以毫秒为单位）。如果默认值不起作用，可根据计算机性能增加此值。
SOL_CLIENT_TX_BUFFERING_TIMEOUT	100	客户端传输缓冲超时值（以毫秒为单位）。这是客户端在发送缓冲的传输字节前等待传输缓冲区变满的时间值。值 0 表示客户端仅在缓冲变满时传输数据。 最小值：0 最大值：65535 默认值：100
SOL_CLIENT_TX_OVERFLOW_TIMEOUT	0	客户端传输溢出超时值（以毫秒为单位）。这是客户端在开始丢弃传输字节前等待传输缓冲区变满的时间值。值 0 表示无超时。 最小值：0 最大值：65535 默认值：0

表 5　**configuration.properties** 文件中的配置参数 （续）

参数	默认值	描述
SOL_CLIENT_HB_INTERVAL	5000	客户端检测信号间隔 （以毫秒为单位）。这是客户端两次将检测信号消息发送到 HPCA Server （以指示客户端仍在运行）之间的等待时间值。值 0 表示不发送检测信号。在这种情况下， HPCA Server 不会监视来自客户端的接收活动，因此无法确定其是否在运行。 最小值：0 最大值：65535 默认值：5000
SOL_CLIENT_RX_TIMEOUT	10000	客户端接收超时值 （以毫秒为单位）。如果此时间值已到，而客户端还没有从 HPCA Server 接收到任何消息，客户端将关闭 SOL 会话。当 SOL 会话打开时，HPCA Server 将定期发送检测信号消息，以确保客户端接收超时值不会逾期 （HPCA Server 检测信号消息之间的间隔时间基于客户端接收超时值）。 最小值：10000 最大值：65535 默认值：10000

表 5　**configuration.properties** 文件中的配置参数 （续）

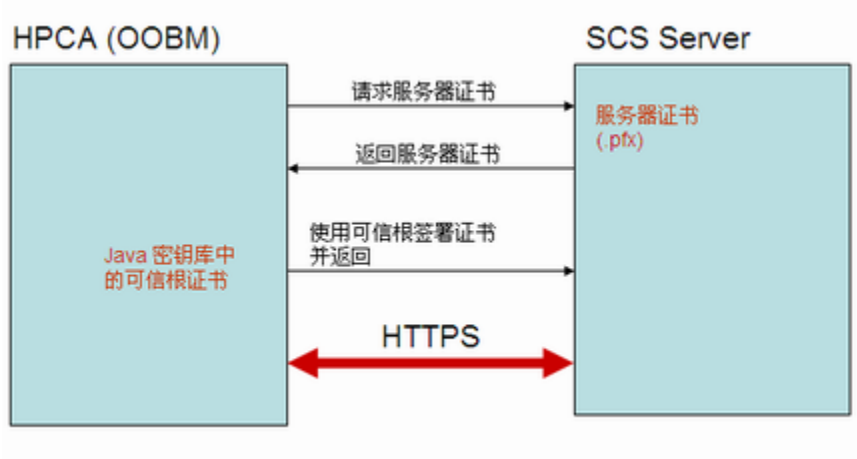
参数	默认值	描述
SOL_CLIENT_FIFO_RX_FLUSH_TIMEOUT	100	客户端清除 FIFO 接收超时值 （以毫秒为单位）。这是客户端在清除接收到的数据前等待 FIFO 接收缓冲区变满的时间值。值 0 表示客户端在操作系统不读取接收到的数据时从不清除数据。 最小值：0 最大值：65535 默认值：100 （HPCA Server 的内部默认值为 0。建议不要使用 100 以下的值。值 0 会导致客户端不清除接收到的数据。因此，如果缓冲区溢出，客户端将取消会话。）
SOL_THREADS_SLEEP_TIME	500	SOL 线程休眠时间
USB_BOOT_SOURCE_VALUES	USB	USB 的引导源名称
WSMAN_MAX_ENUMERATION_RECORDS	5	单次 WSMAN 枚举或请求调用可以获取的最大元素数
WSMAN_TIMEOUT	30000	WSMAN 调用超时（WSMAN 调用等待响应的最大毫秒数）
DEVICE_DELETED_IN_SINGLE_QUERY	30	用于对多个设备执行删除操作的单个 SQL 查询。

➤ 您为 `*BOOT_SOURCE_VALUES` 参数指定的值将用于 HPCA Server GUI，以便为这些引导设备提供用户友好的名称。如果不提供这些参数的值，则可能会看到一些非直观的文本字符串，用以表示这些引导设备。提供的字符串值必须基于 DASH 设备的引导源输出。例如，如果引导源输出为 `BRCM:CD/DVD:3`，用户必须将引导源指定为 **CD/DVD**（而*非* CD），才能在 GUI 中看到 CD/DVD。

配置 OOBM 服务和 SCS 之间的安全访问

您可以用此相同的服务器证书在 SCS Server 和 HPCA Server 上运行的 OOBM 服务之间提供安全通信。为确保这两个组件之间的通信安全，必须导出 SCS Server 上的 Microsoft CA 可信根证书，并将其导入 HPCA Server 上的 Java 密钥库中，这样 HPCA Server 就可以签署服务器证书以验证 SCS Server。

图 2　OOBM 和 SCS 之间的安全访问



如果您已经按导出根证书（第 20 页）中所述，作为 TLS 相互验证设置的一部分导出根证书，则不必再执行此任务。

若要导出根证书，请按导出根证书 （第 20 页）中的步骤执行。

要将根证书导入到 Java 密钥库，请按将根证书导入 Java 密钥库 （第 46 页）中的步骤执行。

禁用 OOBM 服务和 SCS 之间的安全访问

安装并配置 OOBM 后，带外管理服务和 SCS Server 之间的安全超文本传输协议 (HTTPS) 处于启用状态。启用 HTTPS 是鉴于以下原因：

- 已将 SCS 路径配置为使用 HTTPS 作为 OOBM 设备类型设置的一部分，或者已在 `config.properties` 文件中指定。
- 已导出可信根证书，并将其导入 HPCA Server 上的 Java 密钥库。有关详细信息，请参见配置 OOBM 服务和 SCS 之间的安全访问 （第 45 页）。

如果要使用 HTTP 而不是安全传输协议，则可以通过 IIS 管理器禁用 HTTPS。

建议不要这样做。如果禁用 HTTPS，用户凭据将不再加密。它们会以明文传输。

禁用 HTTPS

1 在 SCS 计算机上打开 IIS 管理器。

2 在窗口左手侧的导航面板上，导航到**网站** > **默认网站** > **AMTSCS**。AMTSCS 是 SCS URL 的虚拟目录。

3 右键单击 **AMTSCS**，并从其上下文菜单中选择**属性**。此时将打开 “AMTSCS 属性” 窗口。

4 选择**目录安全**选项卡。

5 在窗口底部的**安全通信**部分，单击**编辑**。此时将打开 “安全通信” 窗口。

6 取消选中窗口顶部的**需要安全通道 (SSL)** 复选框。

7 单击两次**确定**，退出 IIS 管理器。

   在 config.properties 文件中，将 scsserver_url 参数的值更改为在其 URL 中指定 HTTP 协议的值。

8 重新启动 Tomcat 服务。

将根证书导入 Java 密钥库

为了执行 TLS 验证，需要将可信根证书导入 HPCA Server 的 Java 密钥库中。该证书是供 OOBM 验证 vPro 设备用的。您已在导出根证书 （第 20 页）中将此根证书导出为 .cer 文件。

如果已经按配置 OOBM 服务和 SCS 之间的安全访问 （第 45 页）中所述将根证书导入了 HPCA Server 的 Java 密钥库，从而确保 OOBM 和 SCS Server 之间的通信安全，则不必再执行此过程。

将根证书导入 Java 密钥库

1 在 HPCA Server 上，备份现有的可信证书文件。这是 cacerts 文件，通常位于 < *安装目录* >\jre\lib\security。

2 从 JRE 目录运行以下命令。默认 JRE 目录是 C:\Program Files\Hewlett Packard\HPCA\jre\bin。

   keytool -import -noprompt -alias customcacert -keystore ..\lib\security\cacerts -storepass <*store-password*> -file <*ca_file.cer*>

   — *<store-password>* 是证书库的密码。默认情况下，此密码是 **changeit**。

   — *<ca_file.cer>* 是您在导出根证书 （第 20 页）中导出并复制到 HPCA Server 的根证书的完整路径名 （如果该计算机与 SCS Server 计算机不同）。

   此命令将根证书导入 cacerts 库中。

3 通过比较新 cacerts 文件和备份版本的文件大小来验证。新文件要大 1 或 2 KB。

如果应用程序安装在非默认位置，则 cacerts 文件和 JRE bin 目录的位置可能会有所变化。HPCA Server 的默认安装目录是 C:\Program Files\Hewlett Packard\HPCA。

4 停止 Tomcat 服务。

5 从 Tomcat bin 目录运行以下命令。默认 Tomcat bin 目录是 <*安装目录*>\tomcat\bin。

   a **tomcat.exe //US//HPCA-Tomcat ++JvmOptions "-Djavax.net.ssl.keyStore= <*PFX 格式的客户端证书路径*>"**

   b **tomcat.exe //US//HPCA-Tomcat ++JvmOptions "-Djavax.net.ssl.keyStoreType=pkcs12"**

   c **tomcat.exe //US//HPCA-Tomcat ++JvmOptions "-Djavax.net.ssl.keyStorePassword=<*PFX 客户端证书密码*>"**

   *PFX 格式客户端证书路径*和 *PFX 客户端证书密码*与配置安全参数（第 35 页）指定的相同。

6 启动 Tomcat 服务。

将证书转换成 PEM 格式

只有在配置了 TLS 后才需要执行此步骤。

为了在 TLS 打开时能够确保 IDE-R 和 SOL 会话安全，证书在 HPCA Server 上必须是 PEM 格式。根证书已如导出根证书（第 20 页）中所述导出为 .cer 文件。客户端证书已如导出客户端证书（第 20 页）中所述导出为 .pfx 文件。如果 HPCA Server 与导出证书的 SCS Server 不是同一台计算机，则上述文件已复制到 HPCA Console 计算机上。

将根证书转换成 PEM 格式

从 OpenSSL 目录运行以下命令。默认 OpenSSL 目录是 <*安装目录*>\Media\oobm\win32\sca\CertGenerator\OpenSSLHPCA\Media\oobm\win32\sca\CertGenerator\OpenSSL.

Openssl x509 -inform DER -outform PEM -in <*root.cer*> -out <*root.pem*>

其中 <*root.cer*> 是 .cer 格式的 Microsoft CA 服务器根证书，<*root.pem*> 是 .pem 格式的 Microsoft CA 服务器根证书。

示例：

```
Openssl x509 -inform DER -outform PEM -in C:\SCS\RootCA.cer -out
C:\SCS\RootCA.pem
```

将客户端证书转换成 PEM 格式

从 OpenSSL 目录运行以下命令。默认 OpenSSL 目录是 <*安装目录*>\Media\oobm\win32\sca\CertGenerator\OpenSSLHPCA\Media\oobm\win32\sca\CertGenerator\OpenSSL.

Openssl pkcs12 -in <*client.pfx*> -out <*client.pem*>

<*client.pfx*> 是导出到 HPCA Server 的 .pfx 格式的客户端证书， <*client.pem*> 是导出到 HPCA Server 的 .pem 格式的客户端证书 （由 .pfx 格式转换而来）。

示例：

```
Openssl pkcs12 -in C:\SCS\ClientAuth.pfx -out C:\SCS\ClientAuth.pem
```

4 管理任务

本章描述您需要以管理员角色执行以便准备好管理 OOB 设备的配置任务。 HPCA Console 的**配置**选项卡上将提供所有这些任务。它们包括以下内容：

- 启用
- 设备类型选择
- vPro 系统防御设置
- 执行置备任务

为获得 HPCA Console 的最佳查看效果，请将显示控制台的屏幕分辨率设为 1280x1024。

启用

要执行 OOBM 任务，登录到 HPCA Console 时要做的第一件事就是启用带外管理 （如果尚未启用）。

禁用 OOBM 时，HPCA Console 的**配置**和**操作**选项卡上的 OOBM 选项（**启用**除外）不可见。而且，HPCA Console 中的**管理**选项卡中没有可以访问带外设备控制台的选项。

启用 OOBM

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理**下，单击**启用**。此时将打开 “启用” 窗口。

3 选中**启用**旁的复选框，然后单击**保存**。带外管理将启用。您将自动注销。

4 登录到 HPCA Console。

重新登录到 HPCA Management Console 后，将看到在以下配置、操作和管理部分中描述的其他 OOBM 选项。

配置

除了**启用**，在**配置**选项卡上的**带外管理**下，您将看到**设备类型选择**。

根据您的设备类型选择，可能还显示其他选项。有关详细信息，请参见vPro 系统防御设置（第 53 页）。

操作

带外管理现在在**操作**选项卡上的左导航窗格中可见。

设备类型选择确定在带外管理下显示哪些选项。

管理

现在，将可以直接从 HPCA Console 的**管理**选项卡访问带外设备详细信息。

这是除了第 5 章，设备管理和第 6 章，组管理所述的通常使用**操作**选项卡访问此信息之外的另一种访问方式。

Client Automation Enterprise

在 CAE 中，从**管理**选项卡访问 “带外设备详细信息” 有多种方式。

使用 “设备” 下拉菜单的设备

1 在**目录**下，展开 **Zone**，然后单击 **Devices**。此时将打开 “目录对象” 窗口。

2 从设备名称旁的下拉菜单，选择**带外设备详细信息**。如果设备支持 OOBM，则 “带外设备详细信息” 窗口将打开。否则，将显示错误消息。

使用 “带外设备详细信息” 图标的设备

1 在**目录**下，展开 **Zone**，然后单击 **Devices**。此时将打开 “目录对象” 窗口。

2 单击设备名称链接。在 “信息” 部分上的工具栏中，“带外设备详细信息” 图标显示。

3 在 “设备” 表中选择设备，然后单击 。如果设备支持 OOBM，则 “带外设备详细信息” 窗口将打开。否则，将显示错误消息。

使用 “查看 / 编辑属性” 图标的设备

1 在**目录**下，展开 **Zone**，然后单击 **Devices**。此时将打开 “目录对象” 窗口。

2 单击设备名称链接。在 “信息” 部分上的工具栏中，“查看 / 编辑属性” 图标显示。

3 单击 。在 “目录对象” 窗口为特定设备打开的工具栏中，“带外设备详细信息” 图标显示。

4 单击 。如果设备支持 OOBM，则 “带外设备详细信息” 窗口将打开。否则，将显示错误消息。

通过组的设备

1 在**目录**下，展开 **Zone**，然后单击 **Groups**。此时将打开 “目录对象” 窗口。

2 选择任意包含设备的组。此时将打开 “目录对象” 窗口，在所选组中显示设备。

您可以使用上述任意设备过程，即使用 “设备” 下拉菜单的设备、使用 “带外设备详细信息” 图标的设备和使用 “查看 / 编辑属性” 图标的设备来访问 “带外设备详细信息” 窗口。

Client Automation Standard

在 CAS 中，从**管理**选项卡访问 “带外设备详细信息” 有多种方式。

使用 “带外设备详细信息” 图标的设备管理

1 在左导航窗格中的**管理**选项卡上单击**设备管理**。将打开 “设备管理” 窗口。

2 选择**设备**选项卡。在 “设备” 表的工具栏中，“带外设备详细信息” 图标显示。

3 在 “设备” 表中选择设备，然后单击 。如果设备支持 OOBM，则 “带外设备详细信息” 窗口将打开。否则，将显示错误消息。

使用设备名称链接的设备管理

1 在左导航窗格中的**管理**选项卡上单击**设备管理**。将打开 “设备管理” 窗口。

2 选择**设备**选项卡。

3 在 “设备” 表中单击设备名称链接。“设备详细信息” 窗口将打开。

4 选择**常规**选项卡。

5 在 “常见任务” > “任务” 下，单击**带外**。如果设备支持 OOBM，则 “带外设备详细信息” 窗口将打开。否则，将显示错误消息。

使用 “带外设备详细信息” 图标的组管理

1 在左导航窗格中的**管理**选项卡上单击**组管理**。此时将打开 “组管理” 窗口。

2 选择**组**选项卡。

3 在 “组” 表中单击组名称链接。此时将打开 “组详细信息” 窗口。

4 选择**设备**选项卡。在 “设备” 表的工具栏中，“查看带外设备详细信息” 图标显示。如使用 “带外设备详细信息” 图标的设备管理中所述继续操作。

使用 “带外设备详细信息” 图标的软件管理

1 在左导航窗格中的**管理**选项卡上单击**软件管理**。“软件管理” 窗口将打开。

2 按照使用 “带外设备详细信息” 图标的组管理内的相同常规步骤，只是在步骤 2 中选择**软件**选项卡。

使用 “带外设备详细信息” 图标的补丁程序管理

1 在左导航窗格中的**管理**选项卡上单击**补丁程序管理**。“补丁程序管理” 窗口将打开。

2 按照使用 “带外设备详细信息” 图标的组管理 （第 51 页）内的相同常规步骤，只是在步骤 2 中选择**补丁程序**选项卡。

使用 “带外设备详细信息” 图标的操作系统管理

1 在左导航窗格中的**管理**选项卡上单击**操作系统管理**。“操作系统管理” 窗口将打开。

2 按照使用 “带外设备详细信息” 图标的组管理 （第 51 页）内的相同常规步骤，只是在步骤 2 中选择**操作系统**选项卡。

设备类型选择

要执行的下个配置任务是选择要管理的 OOB 设备的类型。

选择设备类型

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理**下，单击**设备类型选择**。此时将打开 “设备类型选择” 窗口。

可以选择三个设备类型中的一种：DASH 设备、 vPro 设备或两种设备。

— DASH 设备

要管理 DASH 设备，请选中**管理 Dash 设备**复选框。如果 DASH 管理员将所有 DASH 设备配置为使用相同凭据，可以为这些设备指定公用凭据。

– 对于**所有 DASH 设备使用公用凭据**，选择**是**。“DASH 设备凭据” 字段显示。

– 输入所有 DASH 设备的**用户名**和**密码**。

— vPro 设备

要管理 vPro 设备，请选中**管理 vPro 设备**复选框。将显示 “SCS 属性” 字段。必须输入 SCS 服务的 SCS 登录凭据和 URL。

– 输入 **SCS 服务 URL**。（例如 **http(s)://provisionserver.yourenterprise.com/amtscs**）

– 输入 SCS 管理员的 SCS **用户名**和**密码**。

— 两种设备

要管理 DASH 和 vPro 这两种设备，请选中 DASH 设备的**管理 Dash 设备**复选框，并选中**管理 vPro 设备**复选框。

如果选择了两种设备类型，则可以输入 DASH 设备的公用凭据，且必须输入 SCS 登录凭据及 SCS 服务的 URL 才能访问 vPro 设备。

3 单击**保存**。将保存凭据。

如果在输入时出错或 DASH 或 SCS 管理员已做更改，下次转到 “设备类型选择” 窗口时，将可以重新输入公用凭据或 SCS 凭据。

4 注销后再重新登录到 HPCA Console，查看在反映设备类型选择的**配置**和**操作**选项卡上现已可用的带外管理选项。

通过设备类型选择确定配置和操作选项

在进行设备类型选择之后，您将在**配置**和**操作**选项卡上看到这些选项，以反映您所做出的选择。具体内容总结在下表中：

表 6 配置和操作选项

	DASH	vPro
配置	没有其他选项	vPro 系统防御设置
操作	设备管理	执行置备任务 , 设备管理 , 组管理 , 警告通知

进行或更改设备类型选择后，必须注销并再次登录到 HPCA Console，以便在**配置**和**操作**选项卡的导航面板中看到设备类型的相关选项。

vPro 系统防御设置

在具体管理 vPro 设备和设备组之前，要先定义 vPro 系统防御设置。

仅在选择了 vPro 设备类型时，才会出现此配置选项。系统防御设置不应用于 DASH 设备。

在**配置**选项卡的**带外管理**下，单击 **vPro 系统防御设置**。此时将打开 “vPro 系统防御设置” 窗口。

您可以在管理 vPro 设备时创建网络的常规策略、过滤器、启发和监视程序。

选项包括：

- 管理系统防御过滤器
- 管理系统防御策略
- 管理启发信息
- 管理监视程序

管理系统防御过滤器

可以使用 HPCA Console 在系统防御过滤器储备库中查看、创建、更新和移除 vPro 设备的系统防御过滤器。“系统防御”过滤器可以监控网络上的数据包流量，并可根据数据包匹配的过滤条件丢弃数据包或限制其速率。将会向系统防御策略系统分配防御过滤器，启用前者可保护网络。当其对应的策略变为活动策略时，过滤器将激活。

系统防御过滤器列表的工具栏上的图标使您可以管理这些过滤器。

表 7　系统防御过滤器列表工具栏

图标	功能
	刷新列表中显示的系统防御过滤器
	将系统防御过滤器添加到储备库
	从储备库移除系统防御过滤器

刷新系统防御过滤器视图

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**过滤器**。此时将打开 “过滤器”窗口。其中显示通过 HPCA Console 创建的系统防御过滤器。

3 单击工具栏上的 刷新图标。

添加系统防御过滤器

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**过滤器**。此时将打开 “过滤器”窗口。其中显示通过 HPCA Console 创建的系统防御过滤器。

3 单击工具栏上的 添加图标。“网络过滤器向导”将打开。

4 单击**下一步**继续。此时将打开 “过滤器详细信息”窗口。在此窗口中，指定以下信息：

— **过滤器名称**：输入过滤器的名称。

— **过滤器类型**：选择要创建的过滤器的类型。页面上有对每种类型的解释。

— **每秒的数据包数**：此字段仅在选择了过滤器类型 “速率限制过滤器”时启用。为过滤器输入数据包速率限制。按秒指定数据包速率。

— **与过滤器匹配时创建事件**：如果要创建事件，则选择**是**。事件创建可导致事件写入 vPro 日志和/或事件警告发送到 HPCA Console，具体取决于事件管理器在事件过滤器中查找的条目。

5 单击**下一步**。此时将打开 “参数”窗口。在此窗口中，指定以下信息：

— **数据包类型**：从下拉菜单选择数据包类型。数据包类型可以为 TCP 数据包 (IPv4)、 UDP 数据包 (IPv4)、IP 数据包 (IPv4) 或以太网框架。在此字段中指定的包类型确定将应用过滤器的包报头。

— **下一个协议**：此字段仅当在 “数据包类型”字段中选择了 IP 数据包时显示，因为它仅适用于过滤 IP 数据包。从下拉菜单选择下一个级别数据包协议。下一个级别协议有 TCP、UDP 和 ICMP。这些协议是 TCP/IP 抽象模型的 Internet 层中的更高级别协议。

— **其他协议**：此字段仅当已在 “数据包类型”字段中选择了 IP 数据包时显示，且仅在针对 “下一个协议”选择了 “其他”时启用。可以在 **http://www.iana.org/assignments/protocol-numbers** 处找到其他 IP 协议。

— **TCP 标记**：此标记类型仅当在 “数据包类型”字段中选择了 TCP 数据包时显示，因为它仅适用于过滤 TCP 数据包。检查所需标记类型。可检查的类型数量不受限制。这些标记可选。如果创建 TCP 过滤器，而不指定标记，将匹配所有类型的 TCP 数据包。

— **以太网框架类型**：此字段仅当在 “数据包类型”字段中选择了以太网框架数据包时显示，因为它仅适用于过滤以太网数据包。从下拉菜单选择框架类型。框架类型可以为 IPv4 或 IPv6。

— **其他以太网框架类型**：此字段仅当已在 “数据包类型”字段中选择了以太网框架数据包时显示，且仅在 “以太网框架类型”字段选择了 “其他”时启用。输入备选以太网框架类型。您可以在 **http://www.iana.org/assignments/ethernet-numbers** 处找到不同以太网框架类型。

— **过滤器模式或方向**：选择过滤器模式。此操作指定是由 vPro 设备接收 （接收）数据包还是从 vPro 设备传输 （传输）数据包。

— **网络地址**：此部分仅当在 “数据包类型”字段中选择了 IP、 TCP 或 UDP 数据包时显示，因为它仅适用于过滤 IP、 TCP 和 UDP 数据包。可以选择以下某个选项：

过滤来自 / 发往设备的数据包：此选项使您可以过滤单个设备的数据包。输入远程设备的 IP 地址。如果选择过滤器模式接收，则过滤器将应用于来自此 IP 地址和发往 vPro 设备的数据包。如果选择过滤器模式传输，则过滤器将应用于发往此 IP 地址和来自 vPro 设备的数据包。

过滤来自 / 发往子网的数据包：此选项使您可以过滤某个子网地址范围的数据包。输入 IP 地址和子网掩码。 IP 地址和子网掩码的组合指定过滤的子网地址范围。如果选择过滤器模式接收，则过滤器将应用于来自远程设备的此子网地址范围以及发往 vPro 设备的数据包。如果选择过滤器模式传输，则过滤器将应用于发往远程设备的此子网地址范围以及来自 vPro 设备的数据包。

过滤来自 / 发往网络的数据包：此选项允许过滤整个网络的数据包。如果选择过滤器模式 “接收”，则过滤器将应用于来自所有远程设备和发往 vPro 设备的数据包。如果选择过滤器模式 “传输”，则过滤器将应用于发往所有远程设备和来自 vPro 设备的数据包。

— **端口类型**：此部分仅当在 “数据包类型” 字段中选择了 IP 或 UDP 数据包时显示，因为它仅适用于过滤 TCP 和 UDP 数据包。可以选择以下某个选项：

源端口范围：此选项使您可以指定要应用过滤器的源端口范围 （最小和最大端口值）。将为所有目标端口过滤从此源端口范围传输的数据包。有关详细信息，请参见表 8。

目标端口范围：此选项使您可以指定要应用过滤器的目标端口范围 （最小和最大端口值） 。将为此目标端口范围过滤从所有端口传输的数据包。有关详细信息，请参见表 8。

表 8　端口确定

		过滤器模式	
		从 vPro 设备传输的数据包	**由 vPro 设备接收的数据包**
IP 端口方向	**源端口范围**	参见 vPro 设备上的端口。将过滤从 vPro 设备上此源端口范围到远程目标设备上的所有端口的数据包。	参见远程设备上的端口。将过滤从远程设备上此源端口范围到 vPro 设备上所有端口的数据包。
	目标端口范围	参见远程设备上的端口。将过滤从 vPro 设备上所有端口到远程目标设备上的此端口范围的数据包。	参见 vPro 设备上的端口。将过滤从远程源设备上的所有端口到 vPro 设备上此目标端口范围的数据包。

6　单击**下一步**。显示确认消息。

7　单击**关闭**。新过滤器将在过滤器储备库的 “系统防御过滤器” 表中显示。

更新系统防御过滤器

1　登录到 HPCA Console，并选择**配置**选项卡。

2　在**带外管理 > vPro 系统防御设置**下，单击**过滤器**。此时将打开 “过滤器” 窗口。其中显示通过 HPCA Console 创建的系统防御过滤器。

3　在 “过滤器” 表的 “过滤器名称” 列中单击要修改的过滤器的过滤器名称链接。“网络过滤器向导” 将打开。

4　单击**下一步**继续。根据需要在 “过滤器详细信息” 和 “参数” 页中编辑字段。

5　单击**下一步**。显示确认消息。

6　单击**关闭**。将更新应用于过滤器储备库。

移除系统防御过滤器

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**过滤器**。此时将打开 “过滤器” 窗口。其中显示通过 HPCA Console 创建的系统防御过滤器。

3 选中要从过滤器储备库删除的每个过滤器旁的复选框。

4 单击 删除图标。所选过滤器将从过滤器储备库的 “系统防御过滤器” 表中移除。

您可以使用系统防御过滤器界面：

- 查看可以应用于策略的现有过滤器集合。
- 定义用于隔绝网络病毒感染的过滤器。
- 定义用于转移网络流量以执行各种修复方案的过滤器。
- 定义用于主动监控系统防御数据包的过滤器。
- 移除不再需要的过滤器。

管理系统防御策略

可以使用 HPCA Console 在系统防御策略储备库中查看、创建和移除系统防御策略。然后可以将这些策略部署到网络上的多个 vPro 设备。策略变为活动的时，与此策略关联的过滤器将激活。系统防御策略可以有选择地隔离网络，以避免 vPro 设备受到恶意软件的攻击。

系统防御策略列表的工具栏上的图标使您可以管理这些策略。

表 9　系统防御策略列表工具栏

图标	功能
	刷新列表中显示的系统防御策略
	将系统防御策略添加到储备库
	将系统防御策略部署到 vPro 设备
	取消在 vPro 设备上部署的系统防御策略
	将系统防御和代理程序存在策略分配给有线和无线接口
	从储备库删除系统防御策略

刷新系统防御策略视图

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开 “策略” 窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 单击工具栏上的 刷新图标。

添加系统防御策略

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开 “策略” 窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 单击 添加图标创建新策略。“网络策略向导” 将打开。

4 单击**下一步**继续。在此窗口中，指定以下信息：

— **策略名称**：输入策略的名称。

— **优先级**：输入策略的优先级。数字越大，优先级越高。如果同时启用了系统防御和代理程序存在策略，将使用优先级确定哪个策略将成为活动策略。

— **启用防欺诈过滤器**：选择 “是” 或 “否” 。防欺诈使用传输过滤器。如果启用了此过滤器，它可防止主机用非分配的 IP 地址的源 IP 地址发送 IP 数据包来伪造其身份。

— **默认接收 (Rx) 过滤器类型**：选择 “通过” 或 “丢弃”。默认的接收过滤器将捕获所有不匹配任何其他策略接收过滤器的接收数据包。接收过滤器类型可以为 “通过” 或 “丢弃”。

— **默认传输 (Tx) 过滤器类型**：选择 “通过” 或 “丢弃”。默认的传输过滤器将捕获所有不匹配任何其他策略接传输滤器的传输数据包。传输过滤器类型可以为 “通过” 或 “丢弃”。

5 单击**下一步**。向导的 “过滤器” 页面将打开。

6 从**可用过滤器**列表将要与策略关联的过滤器拖到**要指定给策略的过滤器**列表。

7 单击**添加策略**。显示确认消息。

8 单击**关闭**。新策略将在策略储备库的 “系统防御策略” 表中显示。

更新系统防御策略

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开 “策略” 窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 在 “策略” 表的 “策略名称” 列中单击要修改的策略的策略名称链接。“网络策略向导” 将打开。

4 单击**下一步**。根据需要编辑字段。

5 单击**下一步**可查看当前与策略关联的过滤器。

6 根据您要如何更改所选策略的关联过滤器，将过滤器从一个列表拖放到另一列表。

7 单击**更新策略**。显示确认消息。

8 单击**关闭**。将更新应用于策略储备库。

如果策略已经部署到 vPro 设备，策略将在设备上不更新，仅在储备库中更新。

部署系统防御策略

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开 “策略” 窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 选中要部署的每个策略旁的框。

4 单击工具栏上的 部署图标。此时将打开 “策略部署向导”。

5 单击**下一步**继续。此时将打开 “选择设备” 窗口。

6 选中要部署策略的每个设备旁的框。

7 单击**下一步**。此时将打开 “设置策略” 窗口。使用此窗口可以选择要为所选设备组的有线和无线 NIC 指定的默认系统防御和 / 或代理程序存在策略。相同的策略也可以从系统防御和代理程序存在的每个字段旁的下拉菜单中选择。如果为 NIC （有线或无线）指定了设备上不存在的策略，“结果” 窗口中将显示异常，但这不会影响部署过程。

8 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

9 单击**下一步**继续部署过程。“结果” 窗口将打开，显示部署过程的结果。

10 单击**关闭**退出该向导。

取消部署系统防御策略

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开 “策略” 窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 选中要取消部署的每个策略旁的框。

4 单击工具栏上的 取消部署图标。此时将打开 “取消策略部署向导”。

5 单击**下一步**。此时将打开 “选择设备” 窗口。

6 选中要取消部署策略的每个设备旁的框。

7 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

8 单击**下一步**继续取消部署过程。“结果” 窗口将打开，显示取消部署过程的结果。

9 单击**关闭**退出向导。

设置代理程序存在策略

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 选中要设置为代理程序存在策略的策略旁的框。

4 从 策略管理图标上的下拉菜单中，选择“设置代理程序存在策略（有线 NIC）”。“设置代理程序存在策略向导”将打开。

5 单击**下一步**继续。此时将打开“选择设备”窗口。其中仅显示具有有线 NIC 的可用 vPro 设备。

6 选中要设置所选代理程序存在策略的每个设备旁的框。

7 单击**下一步**。“确认摘要”窗口将打开。在此窗口中检查信息。

8 单击**下一步**继续设置策略过程。“结果”窗口将打开，显示过程的结果。

9 单击**关闭**退出该向导。

10 要为无线 NIC 设置代理程序存在策略，请从设置策略图标下拉菜单中选择“设置代理程序存在策略（无线 NIC）”选项。在这种情况下，“选择设备”窗口将仅显示具有无线 NIC 的可用 vPro 设备。重复对有线 NIC 执行的相同步骤来设置代理程序存在策略。

启用系统防御策略

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 选中要启用为系统防御策略的策略旁的框。

4 从 策略管理图标上的下拉菜单中，选择“启用系统防御策略（有线 NIC）”。“启用系统防御策略向导”将打开。

5 单击**下一步**继续。此时将打开“选择设备”窗口。其中仅显示具有有线 NIC 的可用 vPro 设备。

6 选中要启用所选系统防御策略的每个设备旁的框。

7 单击**下一步**。“确认摘要”窗口将打开。在此窗口中检查信息。

8 单击**下一步**继续启用策略过程。“结果”窗口将打开，显示过程的结果。

9 单击**关闭**退出该向导。

10 要为无线 NIC 启用系统防御在策略，请从设置策略图标下拉菜单中选择“启用系统防御策略（无线 NIC）”选项。在这种情况下，“选择设备”窗口将仅显示具有无线 NIC 的可用 vPro 设备。重复对有线 NIC 执行的相同步骤来启用系统防御策略。

移除系统防御策略

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。其中显示通过 HPCA Console 创建的系统防御策略。

3 选中要删除的每个策略旁的框。

4 单击工具栏上的 删除图标。将显示警告，指出此操作将从储备库删除所选策略，并从所有已置备 vPro 设备上取消部署这些策略。

5 单击**确定**继续。如“系统防御策略”表中所反映出的，这些策略将从储备库移除，并从已置备 vPro 设备取消部署。

您可以使用系统防御策略界面：

- 根据需要定义新系统防御策略。
- 在策略中添加或移除过滤器以进一步优化策略来适应网络的防御需要。
- 根据事件警告和 / 或记录将策略启用为活动的。
- 启用此防欺诈过滤器将使主机无法通过使用与所分配 IP 地址不同的源 IP 地址发送 IP 数据包来伪造身份。
- 移除不再需要的策略。
- 在多个 vPro 设备上部署 （和取消部署）策略。

管理启发信息

您可以使用 HPCA Console 查看、创建、更新、移除和将操作添加到启发信息。然后可以将这些启发部署到多个 vPro 设备。这些启发用于保护网络上的设备，方法是：检测可能出现蠕虫传染的情况并隔离该设备，这样其他的设备就不会受到感染。

启发列表的工具栏上的图标使您可以管理启发规范。

表 10　启发列表工具栏

图标	功能
	刷新列表中显示的启发
	将启发信息添加到储备库
	将启发信息部署到所选 vPro 设备
	在所选 vPro 设备上取消部署启发信息
	从储备库移除启发信息

刷新启发视图

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开“启发”窗口。其中显示通过 HPCA Console 创建的启发。

3 单击工具栏上的 刷新图标。

添加启发

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开“启发”窗口。其中显示通过 HPCA Console 创建的启发。

3 单击 添加图标创建新启发信息。此时将打开 “启发向导”。

4 单击**下一步**继续。此时将打开 “启发详细信息”窗口。在此窗口中，指定以下信息：

- **设置类型**：如果要使用为快速数据包计数、快速时间计数、慢速数据包计数和慢速时间计数参数提供的默认值，请选择 “默认值” 。这些是 Intel 建议的值。如果要修改这些值，请选择“自定义”。请注意，如果更改这些值，可能引起严重网络问题。
- **参数**
  - **名称**：输入启发规范的唯一名称。
  - **快速数据包计数**：如果未选择 “默认”设置类型，请输入快速蠕虫入侵的阈值。阈值 （数据包计数）是一个限制值，当计数器超过此值时，表明有异常事件。可配置的阈值范围为 8 到 64。建议使用 8 作为默认值。
  - **快速时间计数**：如果未选择 “默认”设置类型，请输入快速蠕虫入侵的时间窗口大小。窗口大小 （时间计数）表示启发重置其计数器的时间期间。可配置窗口大小范围为 10 毫秒到 1 秒 （1000 毫秒）。建议使用 10 毫秒作为默认值。
  - **慢速数据包计数**：如果未选择 “默认”设置类型，请输入慢速蠕虫入侵的阈值。阈值 （数据包计数）是一个限制值，当计数器超过此值时，表明有异常事件。可配置的阈值范围为 8 到 64。建议使用 64 作为默认值。
  - **慢速时间计数**：如果未选择 “默认”设置类型，请输入慢速蠕虫入侵的时间窗口大小。窗口大小 （时间计数）表示启发重置其计数器的时间期间。可配置窗口大小范围为 1 秒 （1000 毫秒）到 50 秒 （50000 毫秒）。建议使用 50 秒作为默认值。
  - **遇到超时**：输入的值指定在遇到异常事件时控制操作在多久后应用于 vPro 设备。建议使用 20 和更大的值。如果要永久应用控制操作，请输入值 0。

    有关详细信息，请参见窗口大小和阈值 （第 175 页）和控制操作和超时值 （第 176 页）。

- **操作**
  - **阻止 TX 流量**：从下拉列表中选择**所有 TX 流量**或**仅攻击性端口**。大多数情况下建议使用后一选项 （仅端口流量）
- **策略**
  - **策略名称**：在满足启发条件后，如果要启用系统防御过滤器，请从下拉列表选择策略名称。如果选择了策略，将显示**查看策略信息**链接。如果单击链接，将可以看到策略详细信息。单击**关闭**可关闭策略详细信息窗口。

5 单击**下一步**。此时将显示操作状态。

6 单击**关闭**退出该向导。“启发”表中将显示新的启发信息，且该信息已添加到储备库中。

更新启发

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开“启发”窗口。其中显示通过 HPCA Console 创建的启发。

3 在“启发”表的“启发名称”列中单击要修改的启发规范的启发名称链接。此时将打开“启发向导”。

4 单击**下一步**继续。此时将打开“启发详细信息”窗口。根据需要编辑字段。可以编辑除名称字段外的所有字段。

5 单击**下一步**。此时将显示操作状态。

6 单击**关闭**退出该向导。更新将显示在“启发”表中，并应用于储备库。

如果启发信息已经部署到 vPro 设备，它将在设备上不更新，仅在储备库中更新。

部署启发

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开“启发”窗口。其中显示通过 HPCA Console 创建的启发。

3 选中要部署的每个启发旁的框。

4 单击工具栏上的 部署启发图标。此时将打开“启发向导”。

5 单击**下一步**继续。此时将打开“选择设备”窗口。

6 选中每个要部署启发信息的设备旁边的框。

7 单击**下一步**。此时将打开“启发设置”窗口。

8 选择要应用于所选设备上有线和无线网络接口的启发。可以为这两种接口设置相同的启发信息。如果为 NIC（有线或无线）指定了设备上不存在的启发信息，“结果”窗口中将显示异常，但这不会影响部署过程。

9 单击**下一步**。“确认摘要”窗口将打开。在此窗口中检查信息。

10 单击**下一步**继续部署过程。此时将打开 “结果” 窗口，显示操作结果。

11 单击**关闭**退出该向导。

取消部署启发

1 登录到 HPCA Console，并选择 “配置” 选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开 “启发” 窗口。其中显示通过 HPCA Console 创建的启发。

3 选中要取消部署的每个启发旁的框。

4 单击工具栏上的 取消部署启发图标。此时将打开 “启发取消部署向导”。

5 单击**下一步**。此时将打开 “选择设备” 窗口。

6 选中要取消部署启发的每个设备旁的框。

7 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

8 单击**下一步**继续取消部署过程。“结果” 窗口将打开，显示取消部署过程的结果。

9 单击**关闭**退出向导。

移除启发

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开 “启发” 窗口。其中显示通过 HPCA Console 创建的启发。

3 选中要删除的每个启发旁的框。

4 单击工具栏上的 删除图标。将显示警告，指出此操作将从储备库删除所选启发，并从所有已置备 vPro 设备上取消部署这些启发。

5 单击**确定**继续。如 “启发” 表中所反映出的，这些启发将从储备库移除，并从已置备 vPro 设备取消部署。

使用 “启发” 界面可以：

- 配置时间窗口大小 （时间计数）和阈值 （数据包计数），以根据启发信息确定蠕虫是否已侵入 vPro 设备。
- 指定满足启发条件时为了控制蠕虫而采取的操作。
- 移除不再需要的启发信息。
- 在多个 vPro 设备上部署 （和取消部署）启发。

管理监视程序

您可以使用 HPCA Console 查看、创建、更新、移除和将操作添加到监视程序储备库中的监视程序。然后可以将这些监视程序部署到网络上的多个 vPro 设备。监视程序对 vPro 设备上存在的 OOBM 代理程序进行监视。如果 OOBM 代理程序的状态有所更改，可以指定监视程序必须进行的操作。此外，您可以创建在代理程序存在策略激活时向控制台显示的自定义系统消息，以及创建 OOBM 代理程序监控的应用程序软件列表。

监视程序列表的工具栏上的图标使您可以管理监视程序。

表 11　监视程序列表工具栏

图标	功能
	刷新列表中显示的监视程序
	将监视程序添加到储备库
	将所选监视程序部署到 vPro 设备
	从 vPro 设备上取消部署所选监视程序
	从储备库删除监视程序
	配置 OOBM 代理程序系统消息和软件列表
	部署 OOBM 代理程序系统消息和软件列表

刷新代理程序存在视图

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 单击工具栏上的 刷新图标。

添加监视程序

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 单击 添加图标创建监视程序。此时将打开 “监视程序向导”。

4 单击**下一步**继续。在此窗口中，指定以下信息：

— **代理程序类型**：选择 OOBM 代理程序或第三方供应商代理程序，以指定您在 vPro 设备上安装哪种代理程序。默认情况下将选择 OOBM 代理程序。

— **名称**：输入监视程序的唯一名称。

— **代理程序 GUID**：输入第三方供应商代理程序的 GUID。如果已经选择 OOBM 代理程序，则灰显此字段，因为 OOBM 代理程序的 GUID 是已知的。

— **检测间隔**：输入从代理程序到监视程序的检测之间的时间。系统提供了一个默认值。

— **启动间隔**：输入在系统启动后代理程序必须将第一个检测发送到监视程序的时间。系统提供了一个默认值。

5 单击**下一步**。此时将打开向导的 “监视程序操作” 页。在此窗口中，指定以下信息：

— **转变状态：**

从：为将触发操作的代理程序选择初始状态。

到：为将触发操作的代理程序选择最终状态。

— **操作：**

对于**代理程序存在策略**，选择 “启用” 或 “禁用” 以指定如果本地代理程序转变为指定状态或转变为非指定状态，是启用还是禁用代理程序存在策略。如果启用策略，且它比已启用的系统防御策略优先级更高，那么它将变为活动策略。

对于**事件创建**，选择 “启用” 或 “禁用” 可指定在指定的代理程序转变发生时，是否创建事件。如果启用事件创建，则将在设备的 vPro 日志中记录事件，并 / 或向 HPCA Console 发送事件警告，具体取决于事件过滤器处理和警告订阅。

6 单击**添加操作**。操作将添加到窗口底部的 “操作” 表。您可以按不同有效转变状态的定义，在监视程序中添加任意数量的操作。

7 单击**保存**。屏幕上将显示确认消息。

8 单击**关闭**退出该向导。新监视程序将在 “监视程序” 表中显示，并显示正确设置的操作计数。监视程序和操作将应用于储备库。

更新监视程序

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 在 “监视程序” 表的 “监视程序名称” 列中单击要修改的监视程序的监视程序名称链接。此时将打开 “监视程序向导”。

4 单击**下一步**继续。根据需要编辑字段。

5 单击**下一步**。此时将打开向导的 “监视程序操作” 页。在此窗口中，可以添加更多操作或移除现有操作。

— 按照添加监视程序 （第 65 页）中的步骤 5添加操作。

— 通过在窗口底部取消选中要移除的每个监视程序操作旁的框，然后单击 删除图标，来移除操作。

6 单击**保存**。屏幕上将显示确认消息。

7 单击**关闭**退出该向导。更新将显示在 “监视程序” 表中，并应用于监视程序储备库。

如果监视程序已经部署到 vPro 设备，监视程序将在设备上不更新，仅在储备库中更新。

部署监视程序

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 选中要部署的每个监视程序旁的复选框。只能部署一个 OOBM 代理监视程序。可以部署多个第三方代理监视程序，为 vPro 设备上运行的每个第三方代理程序部署一个。

4 单击工具栏上的 部署监视程序图标。此时将打开 “监视程序部署向导”。

5 单击**下一步**继续。此时将打开 “选择设备” 窗口。

6 选中要部署监视程序的每个设备旁的框。

7 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

8 单击**下一步**继续部署过程。此时将打开 “结果” 窗口，显示操作结果。

9 单击**关闭**退出该向导。

取消部署监视程序

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 选中要取消部署的每个监视程序旁的复选框。

4 单击工具栏上的 取消部署监视程序图标。此时将打开 “监视程序取消部署向导”。

5 单击**下一步**。此时将打开 “选择设备” 窗口。

6 选中要取消部署监视程序的每个设备旁的复选框。

7 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

8 单击**下一步**继续取消部署过程。“结果” 窗口将打开，显示取消部署过程的结果。

9 单击**关闭**退出向导。

移除监视程序

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 选中要删除的每个监视程序旁的复选框。

4 单击工具栏上的 删除图标。将显示警告，指出此操作将从储备库删除所选监视程序，并从所有已置备 vPro 设备上取消部署这些监视程序。

5 单击**确定**继续。如 “监视程序” 表中所反映出的，这些监视程序将从储备库移除，并从已置备 vPro 设备取消部署。

配置系统消息和软件列表

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 单击 OOBM 代理程序设置图标。此时将打开 “软件列表” 对话框。

4 在系统消息文本框中，输入要在代理程序存在策略激活后，在 vPro 设备控制台显示的系统消息。提供了默认消息，此消息可以编辑。

5 在软件名称框中，输入 vPro 设备上运行的、需要 OOBM 代理程序监控的安全应用程序名称。例如，可以输入 **`symantec.exe`**。

> 仅扩展名为 `.exe` 的应用程序可供监控。此产品不支持监控任何其他类型的可执行文件。

6 单击**添加**。您可以重复此过程，以创建需要 OOBM 代理程序监视的软件应用程序列表。

7 单击**保存**。此时屏幕上会显示通知消息。

8 单击**关闭**退出该对话框。系统消息和代理程序软件列表将存储在 XML 储备库中。

部署系统消息和软件列表

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开 “监视程序” 窗口。其中显示通过 HPCA Console 创建的监视程序。

3 单击 部署软件列表和系统消息图标。此时将打开 “软件部署向导”。

4 单击**下一步**。此时将打开 “软件标题” 窗口。

5 选择需要 OOBM 代理程序监控的软件应用程序。

6 单击**下一步**。此时将打开 “设备” 窗口。

7 选择要部署列表和消息的设备。

8 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

9 单击**下一步**继续。此时将打开 “结果” 窗口，显示操作结果。

10 单击**关闭**退出该向导。系统消息和应用程序软件列表将写入目标 vPro 设备上的第三方数据存储 (3PDS)。通过在 “设备管理” 窗口中单击设备的主机名，然后在**诊断**部分下，转到**设备资产 > 软件信息 > 已注册应用程序 > HPCA > HPCABlock**，可以查看特定 vPro 设备的此信息。

> 由于软件应用程序列表将写入 vPro 设备上的 3PDS，OOBM 代理程序将从 3PDS 读取列表，如果重新部署修改过的列表，则必须停止并重新启动该设备上的 OOBM 代理程序。

使用 “监视程序”界面可以：

- 定义监视程序监控 vPro 设备上的 OOBM 代理程序。
- 在 OOBM 代理程序受监视程序监控时，为其配置检测速率和启动间隔。
- 移除不再需要的监视程序。
- 在多个 vPro 设备上部署 （和取消部署）监视程序。
- 自定义和部署代理程序存在策略激活时在 vPro 设备的控制台上显示的系统消息以及软件应用程序主列表，可从此列表中选择需要 OOBM 代理程序在目标 vPro 设备上监控的自定义应用程序列表。

这是在**配置**选项卡中执行的最后一个管理任务，使 HPCA Console 准备就绪，从而管理 OOB 设备。

这样，如果您的角色是操作员或管理员，可以访问**操作**选项卡，并开始管理网络中的 OOB 设备。

执行置备任务

HPCA Console 中**操作**选项卡上的带外管理选项之一是 **vPro 置备**。

除非已选择管理 vPro 设备，否则该选项不会存在于 HPCA Console 中。

此选项允许在 vPro 设备上执行多个置备任务。这些包括置备、重新置备以及部分取消置备和全部取消置备。可能需要在管理网络的过程中重新置备或取消置备某些 vPro 设备。这样做的原因包括：

- 重新置备：完整重新置备 vPro 设备。如果已经在 vPro 设备上更改了多个参数，则使用此选项。
- 部分取消置备：仅从 vPro 设备删除 PID 和 PPS。SCS Server 信息（IP 地址和主机名）未更改且只需更改密钥时，则使用此选项。
- 全部取消置备：从 vPro 设备删除所有置备信息。如果 SCS Server 的 IP 地址和名称已经更改，则使用此选项。它允许清除所有内容，然后进行全新的置备。

要执行任何置备任务，必须首先执行以下操作：

- 在 vPro 设备上安装 OOBM 代理程序 （如果尚未安装）。有关详细信息，请参见安装 OOBM 代理程序 （第 26 页）。
- 如果网络安全策略需要包含其他安全性，则返回到 SCS 设置中，并启用一次性密码 (OTP)。有关详细信息，请参见创建和配置配置文件 （第 22 页）。

置备 vPro 设备

1 登录到 HPCA Console，并选择**操作**选项卡。

2 在**带外管理**下，单击 **vPro 置备**。此时将打开 “vPro 置备” 窗口。

3 如果设备表中没有显示设备，则单击工具栏上的 发现图标。此时将打开“vPro 发现”窗口。

4 输入 Active Directory (AD) 的登录凭据以及 AD 服务器的完全限定域名 (FQDN)。这是必需的，因为 HPCA Console 与 AD 通信以获取该特定域中设备的列表。

例如，如果 AD 主机的信息如下：

域名：oobm.hp.com

域用户：Administrator

域密码：password

域主机名：DomainSystem.oobm.hp.com

在字段中输入以下信息：

用户名：`Administrator` （唯一可接受格式）

密码：`password`

FQDN：`DomainSystem.oobm.hp.com` （不接受 IP 地址或主机名）

5 单击**发现**以启动发现过程。单击**取消**以停止发现过程。在发现完成或取消时，您将返回到“vPro 置备”窗口。

设备列表同时显示设备置备状态 （vPro 状态），即已置备、未置备或置备中。而且，还显示 vPro 设备的 UUID 以及 vPro 设备上 OOBM 代理程序的状态。

➤ 不为未置备、置备中和某些完全置备的设备显示 UUID。这是正常行为。

6 选择要置备的设备。

7 单击工具栏上的 置备图标。此时将打开 “远程配置向导”。

8 在 “简介”窗口中，单击**下一步**继续。此时将打开 “配置文件”窗口。

9 在 “配置文件”窗口中，选择要用于置备 vPro 设备的配置文件。

10 单击**下一步**。此时将打开 “摘要”窗口。在此窗口中检查信息。

11 单击**下一步**以确认。此时将打开 “完成”窗口，显示操作结果。

12 单击**关闭**以退出向导，并返回到 vPro 窗口。将在设备列表中更新所选 vPro 设备的状态。

重新置备 vPro 设备

1 在**带外管理**下，单击 **vPro 置备**。此时将打开 “vPro 置备”窗口。

2 单击工具栏上的 置备任务图标，并从其下拉列表选择**重新置备**。

3 要跟踪操作的成败，请单击 置备任务图标，并从其下拉列表中选择**置备状态日志**。操作的状态显示在日志中。

部分取消置备 vPro 设备

1 在**带外管理**下，单击 **vPro 置备**。此时将打开 “vPro 置备”窗口。

2 单击工具栏上的 置备任务图标，并从其下拉列表选择**部分取消置备**。

3 要跟踪操作的成败，请单击 置备任务图标，并从其下拉列表中选择**置备状态日志**。操作的状态显示在日志中。

全部取消置备 vPro 设备

1 在**带外管理**下，单击 **vPro 置备**。此时将打开 “vPro 置备”窗口。

2 单击工具栏上的 置备任务图标，并从其下拉列表选择**全部取消置备**。

3 要跟踪操作的成败，请单击 置备任务图标，并从其下拉列表中选择**置备状态日志**。操作的状态显示在日志中。

5 设备管理

本章说明如何通过 HPCA Console 管理 OOB 设备。不管 OOB 设备的电源状态、操作系统状况如何或是否存在管理代理程序，都可以对其进行管理。

HPCA Console 中的**操作**选项卡上的带外管理选项之一是**设备管理**。此选项允许：

- 管理多个设备
- 管理单个设备

管理多个设备

通过在 “设备管理” 窗口中显示的设备列表中选择相关设备，可以一次在多个 OOB 设备上执行管理任务。

管理多个设备时，可以通过以下操作指定显示的设备及其在设备列表中的排序方式：

- 根据搜索条件搜索特定设备
- 为了更方便地查看，选择一次可显示的设备数以只看到设备子集
- 根据列标题对设备排序

设备列表的工具栏上的图标使您可以同时管理多个 OOB 设备。此表中的一些图标仅与 vPro 设备相关。查看下表中的功能描述，了解每个设备类型可使用哪些操作。

表 12 “设备列表” 工具栏

图标	功能
	用 OOBM 中存储的信息刷新列表中显示的 OOBM 设备信息
	用每个设备上当前存储的设备信息同步列表中显示的所选或所有设备
	发现网络上的 OOB 设备
	管理所选 OOB 设备的开启 / 关闭和重新启动
	管理所选 vPro 设备的警告订阅
	管理 vPro 设备的常见实用程序

表 12 “设备列表”工具栏 （续）

图标	功能
	将系统防御策略部署至所选 vPro 设备
	将启发蠕虫病毒控制信息部署至所选 vPro 设备
	将监视程序部署到选定的 vPro 设备
	将代理程序软件列表和系统消息部署至所选 vPro 设备
	从 OOBM 数据库删除所选设备

第一次登录到 HPCA Console 时，可能必须单击多次 刷新图标，才能看到窗口中显示的被管设备列表。

如设备列表工具栏表中所示， 发现图标允许您手动发现网络上的 OOB 设备。对于 vPro 设备，它可以是完整或增量发现，如设备发现中所述。除了手动发现以外，OOBM 可以按固定时间间隔自动发现设备。此时间间隔可在 `config.properties` 文件（位于 `<HPCA_Install_DIR>\oobm\conf\` 目录）中配置，方法是将 `device_synchronization_timeperiod` 参数设置为新值。同步时间间隔的默认值为零，表示不会自动同步。如果希望自动同步，请将新值设为非零值。此值的单位是分钟。 OOBM 执行自动发现时，它将执行增量发现。对于新发现的设备， OOBM 将从每个设备检索设备信息。

设备发现

工具栏上的 发现设备图标可用于发现网络上的 OOB 设备。

对于启用 DASH 的设备，必须在 HPCA Console 中指定 IP 地址 / 主机名信息或 Active Directory 信息。对于 vPro 设备，必须指定要进行完整还是增量设备发现。vPro 设备随后从 SCS 储备库的设备列表中读取。

发现设备

1 登录到 HPCA Console，选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理”窗口。

3 单击 发现设备图标。此时将打开 “设备发现向导”。

4 单击**下一步**以继续，“发现选项”窗口将打开。

5 在 HPCA Console 的**配置**选项卡上选择的设备类型决定了在此页上显示的发现选项。如果已选择两种设备类型，则会看到以下所有选项；否则将看到其中一个。

对于 DASH 设备：

如果单击**发现 DASH 设备**单选按钮，则会看到可以输入 IP 地址和 / 或主机名或 Active Directory (AD) 信息的选项。

— **使用 “手动输入” 发现 DASH 设备**：指定主机信息时，可以提供多个 IP 地址的逗号分隔列表和要发现的那些设备的主机名。

— **使用 Active Directory 发现 DASH 设备**：要自动从 AD 导入设备，必须输入 **LDAP 主机**（Active Directory 服务器的主机名或 IP 地址）、 **LDAP 端口** （386 是默认端口）、**用户标识**、**密码** （具有管理权限的用户的 Active Directory 凭据）和**要查询的 DN** （Active Directory 中要查询的域名列表）。

例如，如果 AD 主机的信息如下：

域名：oobm.hp.com

域用户：Administrator

域密码：password

端口：386 （默认）

域主机名：DomainSystem.oobm.hp.com

假定计算机列表在 AD 中的 “computers” 节点中。

在字段中输入以下信息：

LDAP 主机：`DomainSystem.oobm.hp.com`

LDAP 端口：`386`

用户标识：`Administrator@oobm.hp.com`

密码：`password`

要查询的 DN：`cn=computers, dc=oobm, dc=hp, dc=com`

➤ 仅当有大量 DASH 设备需要管理时选择 Active Directory (AD) 机制。 AD 发现机制十分耗时，对于几百台设备要很久才能完成。作为 AD 发现的一部分，HPCA Console 调用每台设备，以识别哪些是 DASH 设备。如果设备不可用，管理控制台将等待一段超时期间，从而增加了通过 AD 发现机制发现设备所需的时间。为了更加高效，如果要发现的设备较少，则使用手动发现方法。

对于 vPro 设备：

如果单击**发现 vPro 设备**单选按钮，您会看到可以选择完整或增量发现的选项。

— **发现所有 vPro 设备**：指定此选项会使 OOBM 发现网络上的所有 vPro 设备。

— **发现已更新的 vPro 设备**：指定此选项会使 OOBM 只发现自上次发现过程以来新增或修改过的 vPro 设备。此选项能极大地改进性能，但不会告知您自上次发现过程以来从网络移除的 vPro 设备。

6 单击**下一步**。此时将打开 “摘要” 窗口。它显示有关您输入的发现信息的摘要信息。

7 单击**下一步**继续。此时将打开 “完成” 窗口，显示操作状态。如果无法发现特定 DASH 设备，它会指出来。如果已经尝试通过手动输入 IP 地址或主机名发现设备，将显示特定消息，说明无法发现设备的原因。

8 单击**关闭**退出该向导。在**设备**选项卡上的设备列表中，会显示新发现的设备。如果没有立即看到新发现的设备，则单击工具栏上的 图标。

可以使用此功能方便地发现网络上的 OOB 设备，以便随后可以通过 HPCA Console 管理它们。

多个设备选择

可以同时在多个设备上执行设备管理操作。

选择多个设备

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 通过选中要访问的 OOB 设备的复选框，或选中左上方的 “全选” 复选框，来选择设备。可以基于某些条件搜索设备，并将设备排序以方便选择。

DASH 设备管理的凭据

要管理 DASH 设备，配置设备时必须输入指定的用户名和密码。这些凭据用于任何种类的管理操作，保护 DASH 设备和 HPCA Console 之间的通信。

DASH 设备可配置为使用通用凭据（所有设备具有相同凭据）或不同的单个凭据。您必须从配置该设备的管理员处获取此信息。

可以决定使用通用凭据还是单独的凭据。您不能对某些设备使用通用凭据而对其他设备使用单独凭据。选择使用通用凭据时，将删除单独的凭据。如果对通用凭据选项选择**否**，则如果存在通用凭据，将删除它们。

如果用通用凭据配置 DASH 设备，可以按设备类型选择（第 52 页）中所述，在 “设备类型选择” 窗口中输入通用凭据。

如果 DASH 设备尚未用通用凭据配置，则第一次尝试访问设备以执行管理操作时，必须输入单独凭据。第一次配置后，将 “记住” 凭据，您无需重新输入它们，除非要更改 DASH 设备的凭据。

为 DASH 设备指定单独凭据

1 登录到 HPCA Console，并选择**配置**选项卡。

2 在**带外管理**下，单击**设备类型选择**。此时将打开 “设备类型选择” 窗口。

3 检查**管理 Dash 设备**。

4 对**所有 DASH 设备使用公用凭据**选择**否**。

5 单击**保存**。

6 选择**操作**选项卡。

7 在**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

8 单击 DASH 设备的主机名链接。“凭据管理” 窗口打开。

9 “凭据管理” 窗口会在您第一次访问 DASH 设备时或更改该设备的凭据时打开。否则它是一次性登录步骤。

10 输入 DASH 设备的**设备用户名**和**设备密码**。

11 单击**提交**。 DASH 设备的 “设备详细信息” 窗口打开。

如果在以后的某一天，要将 DASH 设备重新配置为使用通用凭据，可以返回 “设备类型选择” 窗口并选择**是**。该操作会从 HPCA Console 有效地删除单独的凭据。

刷新设备信息

您可以用网络中的设备上当前存储的设备信息同步 HPCA Console 中显示的设备信息。

刷新设备信息

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 OOB 设备。

2 单击 重新加载设备信息图标。为 HPCA Console 中所选设备显示的设备信息现在将与 OOB 设备上存储的信息同步。

如果在 HPCA OOBM 控制台中没有系统防御策略，则控制台中的摘要表列将对与 “系统防御” 和 “代理程序存在” 功能相关信息的四列显示**不适用**。

建议您不要创建任何系统防御策略，除非确实需要使用系统防御功能。从 vPro 设备检索系统防御信息会严重降低重新加载操作的性能。

电源管理

如果多个用户同时在同一目标 OOB 设备上执行远程电源操作，则会导致系统状态不可预测。例如，如果一个用户执行重新启动任务，同时另一个用户在相同设备上执行关闭任务，将无法确定结果。

多个设备电源管理

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 OOB 设备。

2 从 电源图标下拉菜单选择电源状态。您可以给硬盘通电，或者重新启动硬盘或网络。对单个设备执行电源操作时，有更多选项。此时出现确认消息。

3 如果要继续，则单击**确定**。出现监视过程的进度条。在设备列表表中显示所选设备的新电源状态。在窗口的右下角中创建电源状态链接。可以单击此链接以查看电源管理过程的结果摘要。

可以使用此功能在特定时间有效地打开和关闭多个设备，以节约成本。

警告订阅管理

管理多个设备上的警告订阅

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 vPro 设备。

2 从 警告订阅图标下拉菜单，选择要订阅警告还是取消警告订阅。此时出现确认消息。

3 如果要继续，则单击**确定**。出现监视过程的进度条。它消失时，说明您的订阅已根据所选选项创建或取消。创建订阅后，选中标记出现在设备的 “警告订阅” 列中。取消订阅之后， X 标记出现在设备的 “警告订阅” 列中。

您可以使用此功能订阅和取消订阅至多个设备，这样有关事件的警告就可以发送到 HPCA Console。

常见实用程序的管理

工具栏上的 常见实用程序图标让您可以如以下各节所述，在 vPro 设备上执行各种日常管理任务。

它们包括：

- 闪存限制重置

所有部署活动都写入置备的 vPro 设备上的第三方数据存储 (3PDS)。此非易失性内存有闪存限制保护机制，以避免此区域遭滥用。执行的操作导致超过此限制时， HPCA Console 上显示以下消息：

获取应用程序块时出错：闪存写操作超限 – 请单击 “重置闪存限制” 选项重置闪存限制

闪存限制重置功能允许您重置闪存的计数器，这样就可以继续执行写入此非易失性内存的活动。

建议您经常重置此限制，避免由于超过 vPro 设备上的 3PDS 的闪存限制，导致部署活动失败。

重置多个 vPro 设备上的闪存限制

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 vPro 设备。

2 从 常见实用程序下拉菜单，选择**重置闪存限制**选项。此时出现确认消息。

3 单击**确定**继续。所选 vPro 设备的第三方数据存储 (3PDS) 中的计数器重置为零。

可以使用此选项重置 3PDS 计数器，后者充当闪存损耗保护机制。如果在同一 vPro 设备上对非易失性内存进行多次读 / 写访问，则可能发生闪存限制异常。重置计数器允许您继续执行使用此非易失性内存的操作。

系统防御策略的部署

将系统防御策略部署到多个设备

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 vPro 设备。

2 单击 系统防御策略部署图标。此时将打开 “策略部署向导”。

3 单击**下一步**继续。此时将打开 “选择策略”窗口。

4 选择要部署的策略。

5 单击**下一步**。此时将打开 “设置策略”窗口。使用此窗口可以选择要为所选设备组的有线和无线 NIC 指定的默认系统防御和 / 或代理程序存在策略。相同的策略也可以从系统防御和代理程序存在的每个字段旁的下拉菜单中选择。如果为 NIC （有线或无线）指定了设备上不存在的策略，“结果”窗口中将显示异常，但这不会影响部署过程。

   无论设备上的 NIC 数量如何，对一台 vPro 设备只能设置一个代理程序存在策略。如果一台 vPro 设备有多个 NIC，并且为每个 NIC 指定了不同代理程序存在策略，则将会应用最近的设置。

6 单击**下一步**。“确认摘要”窗口将打开。在此窗口中检查信息。

7 单击**下一步**继续。此时将打开 “结果”窗口，显示操作结果。

8 单击**关闭**退出该向导。

可以使用此功能方便地将多个系统防御策略部署至多个 vPro 设备，以保护这些系统免受恶意攻击。

启发的部署

将启发部署到多个设备

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 vPro 设备。

2 单击 启发部署图标。此时将打开 “启发部署向导”。

3 单击**下一步**继续。此时将打开 “选择启发” 窗口。

4 选择要部署的启发。

5 单击**下一步**。此时打开 “设置启发” 窗口。

6 选择要应用于 vPro 设备上的有线和无线网络接口的启发。可以为这两种接口设置相同的启发信息。如果为 NIC（有线或无线）指定了设备上不存在的启发信息，“结果” 窗口中将显示异常，但这不会影响部署过程。

7 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

8 单击**下一步**继续。此时将打开 “结果” 窗口，显示操作结果。

9 单击**关闭**退出该向导。

可用此功能将多个启发部署至多个 vPro 设备，以控制受感染设备的蠕虫病毒。

监视程序的部署

将监视程序部署到多个设备

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 vPro 设备。

2 单击 监视程序部署图标。此时将打开 “监视程序部署向导”。

3 单击**下一步**继续。此时将打开 “选择监视程序” 窗口。

4 选择要部署的监视程序。只能部署一个 OOBM 代理监视程序。可以部署多个第三方代理监视程序，为 vPro 设备上运行的每个第三方代理程序部署一个。

5 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

6 单击**下一步**继续。此时将打开 “结果” 窗口，显示操作结果。

7 单击**关闭**退出该向导。

可以使用此功能方便地将多个监视程序部署至多个 vPro 设备，以便在这些系统上监视 OOBM 代理程序。监视 OOBM 代理程序增强了网络的安全性，因为这些代理程序会反过来监视已置备设备上运行的安全软件。如果安全软件停止运行 （无意或有意地用户干预），则监视程序可以警告此事件的系统管理员。

代理程序软件列表和系统消息的部署

将代理程序软件列表和系统消息部署到多个设备

1 如过程选择多个设备 （第 76 页）中所述，选择要管理的 vPro 设备。

2 单击 部署软件列表和系统消息图标。此时将打开 “部署向导”。

3 单击**下一步**。此时将打开 “软件列表” 窗口。

4 选择需要 OOBM 代理程序监控的软件应用程序。

5 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。

6 单击**下一步**继续。此时将打开 “结果” 窗口，显示操作结果。

7 单击**关闭**退出该向导。系统消息和应用程序软件列表将写入目标 vPro 设备上的第三方数据存储 (3PDS)。您可以通过在**设备**选项卡上选择设备来查看特定 vPro 设备的这一信息，然后在**诊断**部分下面，转到**设备资产** > **软件信息** > **已注册应用程序** > **HPCA** > **HPCABlock**。

➤ 由于软件应用程序列表将写入 vPro 设备上的 3PDS， OOBM 代理程序将从 3PDS 读取列表，如果重新部署修改过的列表，则必须停止并重新启动该设备上的 OOBM 代理程序。

可以使用此功能在多个 vPro 设备上方便地将 OOBM 代理程序系统消息和软件列表部署到 3PDS。

删除设备

从 OOBM 数据库删除设备

1 选择要删除的设备。有关如何选择多个设备的信息，请参见多个设备选择 （第 76 页）。

2 单击 删除设备图标。将出现以下确认消息：

是否要对所选设备进行删除？

3 单击**确定**继续。

管理单个设备

在 “设备管理” 窗口中显示的设备列表表显示设备电源状态、其主机名和其他属性。

要管理单个设备，请在表的 “设备” 列下面单击其主机名链接。

此时将打开所选设备的管理窗口。此窗口允许您执行以下操作：

- 查看 OOB 设备的电源状态 （第 86 页）。
- 查看 vPro 事件日志 （第 87 页）。
- 查看常规资产信息 （第 88 页）。
- 查看 vPro 常规资产信息 （第 88 页）。
- 查看硬件资产 （第 89 页）。
- 如查看软件应用程序 （第 89 页）中所述，查看以第三方数据存储 (vPro) 注册或位于网络控制器的 NVRAM (DASH) 中的应用程序列表。
- 如更改电源状态 （第 90 页）中所述，执行诸如电源开 / 关和重新启动之类的远程操作。
- 如 vPro 设备上的 KVM 重定向（第 101 页）中所述，在文本或图形模式下执行 KVM 重定向。
- 如管理 vPro 设备上的系统防御过滤器（第 102 页）中所述，查看和删除 vPro 设备上的系统防御过滤器。
- 如管理 vPro 设备上的系统防御策略 （第 103 页）中所述，查看、删除和启用系统防御策略，并在 vPro 设备上设置代理程序存在策略。
- 如管理 vPro 设备上的启发 （第 105 页）中所述，查看和删除 vPro 上的启发信息。
- 如管理 vPro 设备上的监视程序 （第 106 页）中所述，在 vPro 设备上查看和删除监视程序。
- 配置 vPro 设备上的前面板设置 （第 107 页）。
- 重置 vPro 设备上的闪存限制 （第 107 页）。

➤ 请参见表 3 （第 12 页）以清楚地了解每种设备类型支持的管理操作。

查看电源状态

在工作区的**电源状态**区，可以一目了然地看到 OOB 设备的电源状态。

高级配置和电源接口 (ACPI) 定义了几个电源状态。根据主板、BIOS 和操作系统的支持状态，这些状态中某些可能不可用。

电源状态范围可以从 S0 （正常工作状态）到逐渐加深的睡眠状态，直到 S5 （软关机状态）和机械关机状态。 S0 到机械关机状态映射到 G0 到 G3 状态，如下所示：

- G0
  - — S0：唤醒。系统充分供电并运行。不节电。

- G1
  - S1：待机。 CPU 减速，并且关闭某些组件。在 RAM 中维护系统状态。系统几乎可以立即唤醒，但只节约少量电。
  - S2：也是待机。关闭 CPU 与某些组件。在 RAM 中维护系统状态。使用更少电量，但系统唤醒需要更长时间。
  - S3：挂起至 RAM。关闭 CPU 和多数组件。只在 RAM 中维护系统状态。这样能节约更多电量，但增加了唤醒所需时间。
  - S4：休眠。将系统状态 （包括 RAM 内容）保存到非易失性存储器，并且关闭所有组件。该状态可节约大部分能耗，但唤醒时间很长 （取决于 RAM 的大小）。
- G2
  - S5：软关机。操作系统关闭，并且关闭系统。 PC 会在用户指示 PC 关闭时进入此状态。这表示有秩序地关闭。
- G3
  - 机械关闭状态。操作系统关闭，并且（通常用 PSU 后面的开关）断开系统的电源。重新连接时，系统进入 G2 而无需进一步干预。

每个逐渐加深的休眠状态都有更长的唤醒滞后 （最高 G0/S0）以及系统环境的更多损失，但 S4 的环境保存功能除外。S4 是允许在进入休眠之前将环境保存到非易失性存储器的特殊状态，如同在电池电量太低时的情况。 S5 是关闭状况，而机械关闭 (G3) 表示断开电池和外部电源连接。

在 HPCA Console 中，可以在 vPro 和 DASH 设备上执行的电源操作根据下表映射到 ACPI 电源状态：

➤ 并非所有电源操作在两类 OOB 设备上都受支持。查看各种电源操作以清楚了解它相关的设备类型时，请再次参见此表。

➤ DASH 设备的“不支持”可能意味着 DASH 标准不支持电源操作，或者某些硬件供应商不支持它。

表 13　将电源操作映射到电源状态

vPro 电源操作	DASH 电源操作	描述	ACPI 状态
对硬盘驱动器供电	启动 引导源：硬盘	唤醒状态	G0/S0
对本地 CD/DVD 供电	启动 引导源：CD/DVD	唤醒状态	G0/S0
对 IDE-R CD/DVD 供电	不支持	唤醒状态	G0/S0
对 IDE-R 软盘供电	不支持	唤醒状态	G0/S0
对 BIOS Setup 供电	不支持	唤醒状态	G0/S0
对 BIOS Pause 供电	不支持	唤醒状态	G0/S0
对主引导设备供电	不支持	唤醒状态	G0/S0
关闭设备	关闭 （软） 引导源：不适用	软关机状态	G2/S5
重新启动至硬盘驱动器	循环通电 （软） 引导源：硬盘	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
重新启动到本地 CD/DVD	循环通电 （软） 引导源：CD/DVD	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
重新启动至主引导设备	不支持	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）

表 13　将电源操作映射到电源状态 （续）

vPro 电源操作	DASH 电源操作	描述	ACPI 状态
重新启动至 IDE-R CD/ DVD	不支持	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
重新启动至 IDE-R 软盘	不支持	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
重新启动至 BIOS Setup	不支持	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
重新启动至 BIOS Pause	不支持	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
重新启动至 LAN (PXE)	循环通电 （软） 引导源：网络	软关机后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
不支持	不支持	待机状态	S1 或 S2
不支持	挂起 引导源：不适用	挂起状态	S3
不支持	休眠 （软） 引导源：不适用	休眠状态	S4
不支持	关闭 （有序软关机） 引导源：不适用	软关机状态 （之前是执行有序关机的请求）	G2/S5
不支持	关闭 （有序硬关机） 引导源：不适用	机械关机状态 （之前是执行有序关机的请求）	G3

表 13　将电源操作映射到电源状态 （续）

vPro 电源操作	DASH 电源操作	描述	ACPI 状态
不支持	关闭 （硬） 引导源：不适用	机械关闭状态	G3
不支持	循环通电 （有序软通电） 引导源： *<boot_source>*	软关机状态 （之前是执行有序关机的请求），后跟唤醒状态	S0 到 S5，返回 G0/S0（如果丢失 S0 环境信息，则需要进行系统主总线重置或从 POST 和 BIOS 完整引导）
不支持	循环通电 （有序硬通电） 引导源： *<boot_source>*	机械关机状态 （之前是执行有序关机的请求），后跟唤醒状态	G0 到 G3，返回 G0/S0
不支持	循环通电 （硬） 引导源： *<boot_source>*	机械关机状态，后跟唤醒状态	G0 到 G3，返回 G0/S0
不支持	主总线重置 （有序） 引导源： *<boot_source>*	关机状态（硬件重置）（之前是执行有序关机的请求），后跟唤醒状态	G2/S5，返回 G0/S0
不支持	主总线重置 引导源： *<boot_source>*	关机状态（硬件重置），后跟唤醒状态	G2/S5，返回 G0/S0
不支持	诊断中断 引导源： *<boot_source>*	关机状态（硬件重置），后跟唤醒状态	G2/S5，返回 G0/S0

查看 OOB 设备的电源状态

1. 登录到 HPCA Console，然后选择**操作**选项卡。
2. 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。
3. 单击要管理的 OOB 设备的主机名链接。将打开一个管理窗口。
4. 查看窗口左侧的**电源状态**部分下面的信息。

显示的电源状态是最后一个已知状态。这可能不同于当前电源状态。为了确保您看到的是当前电源状态，请务必使用电源状态消息旁边的 刷新图标。

查看 vPro 事件日志

工作区的**诊断**区域允许您查看和清除远程 vPro 设备上的事件日志。被管 vPro 设备上发生的各种事件会导致在 vPro 设备上创建和记录事件。

查看 vPro 事件日志

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**部分下，单击**事件日志**链接。在控制台的内容区域中显示事件日志的内容。您可以看到窗口顶部总结的日志属性。它显示日志中的事件记录数，记录最后一个事件的时间和日志状态 （冻结或解冻） 。冻结日志时，事件不可写入日志。在摘要下面，可以看见事件类型（创建事件的原因）、事件的严重性、记录事件的日期和时间，以及事件的描述。如果在详细信息列中单击 详细信息图标，则打开窗口，显示所选事件的属性详细信息。

5 单击工具栏上的 刷新图标，刷新事件日志视图。

6 单击工具栏上的 清除图标以清除事件日志文件。

7 单击工具栏上的 冻结图标以冻结或解冻事件日志文件，从而更改事件日志的状态。

可以使用事件日志界面：

- 判断是否发生了值得注意、需要立即操作的事件。
- 定期清除日志以确保新事件可以记入。
- 判断 vPro 设备的常规状态或运行状况。

查看 vPro 事件过滤器

工作区的**诊断**区域允许您查看存在于远程 vPro 设备上的默认事件过滤器。事件过滤器确定设备上发生事件时要采取的操作。

查看 vPro 事件过滤器

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**下面，单击**事件过滤器**链接。所选 vPro 设备上存在的默认事件过滤器显示在控制台的内容区域中。

5 单击要查看其详细信息的事件过滤器的名称链接。“事件过滤器详细信息”页打开，显示所选事件过滤器的属性详细信息。

6 单击 刷新图标以刷新事件过滤器。

事件过滤器中的信息可用来帮助您理解所选设备上发生特定类型的事件时，可以采取哪些操作。

查看 vPro 常规资产信息

工作区的**诊断**区域允许您查看有关远程 vPro 设备的常规资产信息，而不论其电源状态或常规运行状况如何。

查看常规资产信息

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理”窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**下面单击**设备资产**链接。

5 单击**常规信息**。

6 单击 **vPro 信息**以查看有关 vPro 设备的常规资产信息。该设备的常规资产信息包括其 IP 地址，侦听端口，置备模式， BIOS 版本等显示在控制台的内容区域中。

7 单击**安全设置**查看与安全性相关的资产信息。该设备与安全相关的信息（包括启用 TLS、加密、SOL、 IDE-R 等）都显示在控制台的内容区域中。

可以使用此信息：

- 检查 vPro 设备的常规资产
- 查看与安全性相关的 vPro 设备的资产信息，看看是否需要采取任何重新配置操作

查看硬件资产

工作区的**诊断**区域允许您在远程 OOB 设备上查看硬件资产。它与操作系统的状态或设备是否通电无关。这减少或消除了手动审核库存的需要，因为您总能找到设备，不管其运行状况或电源状态如何。这一准确地远程查看硬件资产的功能提供了更好的计划性、更高的升级效率、更快的部署速度以及对可现场更换单元 (FRU) 库存的更好管理。

如果 Centrino Pro 笔记本电脑处于关闭、待机或休眠电源模式中，则它无法通过无线网络管理。

查看硬件资产

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 OOB 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**下面单击**设备资产**链接。

5 单击**硬件信息**。

6 单击硬件组件。该组件的规格即会显示在控制台内容区域。

➤ 在某些情况下，您可能看不见 vPro 设备的硬件信息。如果发生这种情况，等待一段时间再重试操作。

可以使用此信息：

- 确定设备上任何可能需要更换的硬件组件的确切规格
- 识别兼容性问题
- 在置备新操作系统之前，请检查其配置
- 检索特别库存信息，即使计算机已关闭。

查看软件资产

工作区的**诊断**区域允许您在启用远程 OOB 的设备上查看软件资产。

对于 vPro 设备，此功能允许您查看 vPro 设备上由 OOBM 代理程序监视的软件应用程序的列表。有关详细信息，请参见管理监视程序（第 64 页）。该列表在该设备上的第三方数据存储 (3PDS) 中注册。

对于 DASH 设备，此功能允许您查看位于该设备的网络控制器的 NVRAM 中的软件库存信息。

查看软件应用程序

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 OOB 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**部分下，单击**设备资产**链接。

5 单击**软件信息**。

6 对 vPro 设备单击**已注册应用程序**，对 DASH 设备单击**已安装软件**。

7 单击应用程序。应用程序的链接允许您查看该应用程序的信息。

可以使用此信息：

- 确定软件应用程序正由 vPro 设备上的 OOBM 代理程序监视。
- 确定安装在 DASH 设备上的软件应用程序。

更改电源状态

您可以从 HPCA Console 执行远程电源管理操作。控制台工作区的**诊断**区域允许您在远程 OOB 设备上更改电源状态。

请参见表 3 （第 12 页）以清楚地了解每种设备类型支持的电源操作。

通过控制台重定向功能，可以在 HPCA Console 上查看电源管理过程，而无须用户干预或离开管理控制台。

在 vPro 设备上， SOL 会话启动 Windows HyperTerminal。退出 HyperTerminal 会话时，将提示您保存配置会话的设置。建议您保存会话设置有两个原因。如果已自定义 HyperTerminal 会话，则会保存它们。而且一旦保存了配置，就不会再次提示您。配置将在用于启动 Web 浏览器以访问 HPCA Console 的计算机上另存为 `.ht` 文件。如果 HyperTerminal 不可用（在 Vista 系统上）或失败，将使用 Telnet。

SOL 向管理控制台提供键盘和文本重定向，*除非*对 vPro 设备上的本地驱动器供电。

通过 TLS 提供此功能的安全性。

在 vPro 设备上还提供 KVM 重定向，用于在图形和文本模式中都提供控制台重定向。 JRE 1.6.x 和 VNC Viewer 必须安装在运行浏览器的计算机上，以便访问 HPCA Console。6.0 版之前，KVM 功能在带有 AMT 的 vPro 计算机上不可用。有关详细信息，请参见 vPro 设备上的 KVM 重定向（第 101 页）。

在通过 BIOS/IDE-R 执行远程操作之前，必须在 HPCA Server 和 vPro 设备上启用 Telnet 服务。默认情况下，`telnet.exe` 存储于 `C:\Windows\System32`。将 `telnet.exe` 复制到其他位置。将 `TELNET_PATH` 系统环境变量设置为 `telnet.exe` 的新路径。如果更改了 `TELNET_PATH` 系统环境变量的值，则必须注销后重新登录系统才能让新值生效。

在 DASH 设备上，如果已在 DASH 设备上安装和配置 SSH PuTTY 客户端，则 HPCA Console 将尝试使用此客户端进行文本控制台重定向。要将设备配置为使用 PuTTY 客户端，必须将 `PUTTY_PATH` 系统环境变量设置为 PuTTY 可执行文件的完整路径，例如 `C:\Putty\putty.exe`。如果更改了 `PUTTY_PATH` 环境变量的值，则必须注销后重新登录系统才能让新值生效。如果 PuTTY 客户端不可用，控制台将使用 Telnet。

对设备供电

1. 登录到 HPCA Console，然后选择**操作**选项卡。
2. 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。
3. 单击要管理的 OOB 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**部分下，单击**远程操作**链接。此时将打开 “远程操作向导” 窗口。

5 单击**下一步**继续。此时将打开 “任务” 窗口。如下表所示，您可以从各种驱动器启动设备，或启动至 BIOS （仅 vPro）。

在 “任务” 窗口中，还可以指定以下内容：

— 对于 vPro 设备，可以指定是否要使用该设备的前面板设置。如果选择**否**，将忽略 vPro 设备的前面板设置。有关详细信息，请参见配置 vPro 设备上的前面板设置 （第 107 页）。

— 对于 DASH 设备，**显示客户端控制台**选项可以用于指定是否要在控制台上显示文本。

在下表中，远程操作受到 vPro 设备或两类 OOB 设备支持时，将使用 vPro 的远程操作的术语。请参见表 3 （第 12 页）以查看 DASH 远程操作的映射。

表 14 设备供电

驱动器 /BIOS	步骤
本地硬盘驱动器	1 从**远程操作**旁边的下拉菜单选择**对硬盘驱动器供电**。 2 单击**下一步**。对于 DASH 设备，将打开 “引导设置” 窗口。在此窗口中，可以指定在引导设备时要使用的引导源或引导配置。选择**硬盘**作为引导源。有关详细信息，请参见配置 vPro 设备上的引导设置 （第 108 页）。 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。管理控制台上将显示摘要信息。 5 单击**关闭**。
本地 CD 驱动器	1 从**远程操作**旁边的下拉菜单选择 **对本地 CD/DVD 供电**。 2 单击**下一步**。对于 DASH 设备，将打开 “引导设置” 窗口。在此窗口中，可以指定在引导设备时要使用的引导源或引导配置。选择 **CD/DVD** 为引导源。有关详细信息，请参见配置 vPro 设备上的引导设置 （第 108 页）。 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。管理控制台上将显示摘要信息。 5 单击**关闭**。

表 14　设备供电（续）

驱动器 /BIOS	步骤
IDE-R CD 驱动器（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**对 IDE-R 供电**。 2 从 **IDE-R 选项**旁边的下拉菜单选择 **IDE-R CD/DVD**。用 CD/DVD 驱动器的默认设置填充“驱动器路径”字段。如果不希望在“驱动器路径”字段中使用默认驱动器，可以指定其他驱动器或管理控制台服务器上的 ISO 文件的路径。如果指定的驱动器路径中的 ISO 文件是共享网络资源，必须使用 UNC 语法，即 `\\hostname\sharefolder\file.iso` 3 单击**下一步**。此时将打开“确认摘要”窗口。在此窗口中检查信息。 4 单击**下一步**继续。将关闭“远程操作向导”，并打开 HyperTerminal 窗口，其中显示了加电过程。此窗口将保持打开，直到您关闭它。
IDE-R 软盘驱动器（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**对 IDE-R 供电**。 2 从 **IDE-R 选项**旁边的下拉菜单选择 **IDE-R 软盘**。用软盘驱动器的默认设置填充“驱动器路径”字段。如果不希望在“驱动器路径”字段中使用默认驱动器，可以指定其他驱动器或管理控制台服务器上的 IMG 文件的路径。如果指定的驱动器路径中的 IMG 文件是共享网络资源，必须使用 UNC 语法，即 `\\hostname\sharefolder\file.img` 3 单击**下一步**。此时将打开“确认摘要”窗口。在此窗口中检查信息。 4 单击**下一步**继续。将关闭“远程操作向导”，并打开 HyperTerminal 窗口，其中显示了加电过程。此窗口将保持打开，直到您关闭它。
BIOS Setup（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**对 BIOS 供电**。显示 **BIOS 选项**。 2 从 **BIOS 选项**旁边的下拉菜单选择 **BIOS Setup**。 3 单击**下一步**。此时将打开“确认摘要”窗口。在此窗口中检查信息。 4 单击**下一步**继续。将关闭“远程操作向导”，并打开 HyperTerminal 窗口，其中显示了加电过程。此窗口将保持打开，直到您关闭它。
BIOS Pause（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**对 BIOS 供电**。显示 **BIOS 选项**。 2 从 **BIOS 选项**旁边的下拉菜单选择 **BIOS Pause**。 3 单击**下一步**。此时将打开“确认摘要”窗口。在此窗口中检查信息。 4 单击**下一步**继续。将关闭“远程操作向导”，并打开 HyperTerminal 窗口，其中显示了加电过程。此窗口将保持打开，直到您关闭它。

表 14　设备供电 （续）

驱动器 /BIOS	步骤
主引导设备（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**对主引导设备供电**。此选项允许您对 vPro 设备的 BIOS 中配置的默认引导设备通电。将显示 **SOL 选项**。此本地引导选项允许您查看 HPCA Console 上显示的操作 （如果您选择这样做）。 2 对于 **SOL 选项**，您可以选择**显示到控制台**或**不显示到控制台**。 3 单击**下一步**。“确认摘要”窗口将打开。在此窗口中检查信息。 4 单击**下一步**。 — 如果您选择了**显示到控制台**，“远程操作向导”将关闭， HyperTerminal 窗口打开，显示通电过程。此窗口将保持打开，直到您关闭它。 — 如果您选择了**不显示到控制台**，将打开摘要信息窗口。它将显示完成操作时的结果。必须单击**关闭**返回到 “设备详细信息”窗口。

关闭设备

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理”窗口。

3 单击要管理的 OOB 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**部分下，单击**远程操作**链接。此时将打开 “远程操作向导”窗口。

5 单击**下一步**继续。

从**远程操作**旁边的下拉菜单选择**关闭设备**。

6 单击**下一步**。此时将打开 “确认摘要”窗口。在此窗口中检查信息。

7 单击**下一步**继续。管理控制台上将显示摘要信息。

8 单击**关闭**。

可以使用此功能：

- 准备管理操作时确认设备的开启 / 关闭
- 准备管理操作时远程打开设备
- 诊断未响应的设备
- 远程重新启动未响应的设备

重新启动系统

工作区的诊断区域允许您重新启动远程 OOB 设备。通过内置重定向功能，您可以查看重新启动过程，而无需用户干预或离开管理控制台。 vPro 设备上的 SOL 和 KVM 向管理控制台提供键盘和视频重定向 （除非对 OOB 设备上的本地设备通电）。

从本地设备重新启动系统

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 OOB 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**诊断**部分下，单击**远程操作**链接。此时将打开 “远程操作向导” 窗口。

5 单击**下一步**继续。此时将打开 “任务” 窗口。如表 15 中所示，可以从 OOB 设备的本地驱动器重新启动设备。

   在 “任务” 窗口中，还可以指定以下内容：

   — 对于 vPro 设备，可以指定是否要使用该设备的前面板设置。如果选择**否**，将忽略 vPro 设备的前面板设置。有关详细信息，请参见配置 vPro 设备上的前面板设置 （第 107 页）。

   — 对于 DASH 设备，**显示客户端控制台**选项可以用于指定是否要在控制台上显示文本。

表 15　从本地驱动器重新启动设备

驱动器	步骤
本地硬盘驱动器	1 从**远程操作**旁的下拉菜单选择**对硬盘供电**。 2 单击**下一步**。对于 DASH 设备，将打开 “引导设置” 窗口。在此窗口中，可以指定在引导设备时要使用的引导源或引导配置。选择**硬盘**作为引导源。有关详细信息，请参见配置 vPro 设备上的引导设置 （第 108 页）。 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。管理控制台上将显示摘要信息。 5 单击**关闭**。

表 15　从本地驱动器重新启动设备 （续）

本地 CD 驱动器	1 从**远程操作**旁边的下拉菜单选择**重新启动至本地 CD/DVD**。 2 单击**下一步**。对于 DASH 设备，将打开 “引导设置” 窗口。在此窗口中，可以指定在引导设备时要使用的引导源或引导配置。选择 **CD/DVD** 为引导源。有关详细信息，请参见配置 vPro 设备上的引导设置 （第 108 页）。 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。管理控制台上将显示摘要信息。 5 单击**关闭**。
主引导设备（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**重新启动到主引导设备**。此选项允许您重新启动至 vPro 设备的 BIOS 中配置的默认引导设备。将显示 **SOL 选项**。此本地引导选项允许您查看 HPCA Console 上显示的操作 （如果您选择这样做）。 2 对于 **SOL 选项**，您可以选择**显示到控制台**或**不显示到控制台**。 3 单击**下一步**。“确认摘要” 窗口将打开。在此窗口中检查信息。 4 单击**下一步**。 — 如果您选择了**显示到控制台**，“远程操作向导” 将关闭，打开 HyperTerminal 窗口，显示重新启动过程。此窗口将保持打开，直到您关闭它。 — 如果您选择了**不显示到控制台**，将打开摘要信息窗口。它将显示完成操作时的结果。必须单击**关闭**返回到 “设备详细信息” 窗口。

可以使用此功能：

- 远程重新启动未响应的设备
- 通过使用控制台重定向查看 BIOS 引导过程，识别引导过程中未响应的失败组件来诊断未响应设备的问题。

重新启动带 IDE-R 的 vPro 系统

工作区的**诊断**区域允许您将有问题 vPro 设备的引导设备重定向到在另一个远程驱动器上的清洁映像。集成的驱动器电子重定向 (IDE-R) 提供此 CD/ 软盘驱动器重定向功能。

➤ 目前仅在 vPro 设备上支持 IDE-R 技术。

vPro 设备通过无线通信与 OOBM 服务器通信需要更长时间。这可能导致 OL/IDE-R 远程操作发生超时。要避免此情况，可以按照配置 IDE-R 和 SOL 超时值 （第 34 页）所述，配置 `IDER*` 和 `SOL*` 参数。

通过内置重定向功能，您可以查看重新启动过程，而无需用户干预或离开管理控制台。vPro 设备的 SOL 和 KVM 向管理控制台提供键盘和视频重定向。

重新启动带 IDE-R 的系统

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧**诊断**部分下，单击**远程操作**链接。此时将打开 “远程操作向导” 窗口。

5 单击**下一步**继续。此时将打开 “任务” 窗口。您可以按下表所示从远程设备上的各种驱动器重新启动带 IDE-R 的 vPro 设备。

   同样是在 vPro 设备的 “任务” 窗口中，可以指定是否要使用 vPro 设备的前面板设置。如果选择**否**，将忽略 vPro 设备的前面板设置。有关详细信息，请参见配置 vPro 设备上的前面板设置（第 107 页）。

表 16　重新启动带 IDE-R 的 vPro 设备

驱动器	步骤
IDE-R CD 驱动器（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**重新启动至 IDE-R**。显示 **IDE-R 选项**。 2 从 **IDE-R 选项**旁边的下拉菜单选择 **IDE-R CD/DVD**。用 CD/DVD 驱动器的默认设置填充 “驱动器路径” 字段。如果不希望在 “驱动器路径” 字段中使用默认驱动器，可以指定其他驱动器或管理控制台服务器上的 ISO 文件的路径。如果指定的驱动器路径中的 ISO 文件是共享网络资源，必须使用 UNC 语法，即 `\\hostname\sharefolder\file.iso` 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。“远程操作向导” 关闭，HyperTerminal 窗口打开，显示重新启动过程。此窗口将保持打开，直到您关闭它。
IDE-R 软盘驱动器（仅 vPro）	1 从**远程操作**旁边的下拉菜单选择**重新启动至 IDE-R**。显示 **IDE-R 选项**。 2 从 **IDE-R 选项**旁边的下拉菜单选择 **IDE-R 软盘**。用软盘驱动器的默认设置填充 “驱动器路径” 字段。如果不希望在 “驱动器路径” 字段中使用默认驱动器，可以指定其他驱动器或管理控制台服务器上的 IMG 文件的路径。如果指定的驱动器路径中的 IMG 文件是共享网络资源，必须使用 UNC 语法，即 `\\hostname\sharefolder\file.img` 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。“远程操作向导” 关闭，HyperTerminal 窗口打开，显示重新启动过程。此窗口将保持打开，直到您关闭它。

可以使用此功能：

- 重新启动非工作设备以临时诊断环境，从而更准确地识别是硬件还是软件问题
- 在非工作设备上重建操作系统映像
- 将操作系统置备为裸机设备
- 捕获设备的图像以供还原或重新部署

重新启动 vPro 系统至 BIOS 设置

工作区的**诊断**区域允许您访问引导前的 BIOS 设置，以便确认配置信息并按需更改设置来帮助解决 vPro 设备问题。

➤ 重新启动到 BIOS 设置的功能仅在 vPro 设备上受支持。

通过内置重定向功能，您可以查看 BIOS 设置，而无需用户干预或离开管理控制台。 vPro 设备的 SOL 和 KVM 向管理控制台提供键盘和视频重定向。

重新启动系统至 BIOS 设置

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧**诊断**部分下，单击**远程操作**链接。此时将打开 “远程操作向导” 窗口。

5 单击**下一步**继续。此时将打开 “任务” 窗口。可以使用下表所示的各种选项重新启动设备到 BIOS 设置。

   同样是在 vPro 设备的 “任务” 窗口中，可以指定是否要使用 vPro 设备的前面板设置。如果选择**否**，将忽略 vPro 设备的前面板设置。有关详细信息，请参见配置 vPro 设备上的前面板设置（第 107 页）。

表 17　重新启动 vPro 设备至 BIOS 设置

BIOS	步骤
BIOS Setup（仅 vPro）	1 从**远程操作**旁的下拉菜单选择**重新启动至 BIOS**。显示 **BIOS 选项**。 2 从 **BIOS 选项**旁边的下拉菜单选择 **BIOS Setup**。 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。“远程操作向导” 关闭，HyperTerminal 窗口打开，显示重新启动过程。此窗口将保持打开，直到您关闭它。
BIOS Pause（仅 vPro）	1 从**远程操作**旁的下拉菜单选择**重新启动至 BIOS**。显示 **BIOS 选项**。 2 从 **BIOS 选项**旁边的下拉菜单选择 **BIOS Pause**。 3 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。 4 单击**下一步**继续。“远程操作向导” 关闭，HyperTerminal 窗口打开，显示重新启动过程。此窗口将保持打开，直到您关闭它。

可以使用此功能：

- 确认配置信息
- 根据需要更改设置，以诊断非工作设备的问题
- 更改 BIOS 设置，而无需实际访问设备

重新启动系统以预引导执行环境

工作区的**诊断**区域允许您重新启动 OOB 设备至预引导执行环境 (PXE)。此重新启动选项允许您使用网络接口卡引导计算机，而不依赖于本地硬盘或已安装的操作系统。OOB 设备可以从 PXE 服务器上的引导映像重新启动。

它假定网络环境中有 PXE 引导服务器。PXE 引导服务器需要设置 DHCP 服务器、TFTP 服务器和引导服务器来处理 PXE 引导请求。

重新启动系统到 PXE

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧**诊断**部分下，单击**远程操作**链接。此时将打开 “远程操作向导” 窗口。

5 单击**下一步**继续。此时将打开 “任务” 窗口。

6 从**远程操作**旁的下拉菜单选择**重新启动至 LAN (PXE)**。

   在 “任务” 窗口中，还可以指定以下内容：

   — 对于 vPro 设备，可以指定是否要使用该设备的前面板设置。如果选择**否**，将忽略 vPro 设备的前面板设置。有关详细信息，请参见配置 vPro 设备上的前面板设置 （第 107 页）。

   — 对于 DASH 设备，**显示客户端控制台**选项可以用于指定是否要在控制台上显示文本。

7 单击**下一步**。对于 DASH 设备，将打开 “引导设置” 窗口。在此窗口中，可以指定在引导设备时要使用的引导源或引导配置。选择**网络**作为引导源。有关详细信息，请参见配置 vPro 设备上的引导设置 （第 108 页）。

8 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。

9 如果要继续，则单击**下一步**。管理控制台上将显示摘要信息。

10 单击**关闭**退出该向导。

可以使用此功能：

- 重新启动非工作设备以临时诊断环境，从而更准确地识别是硬件还是软件问题
- 在非工作设备上重建操作系统映像
- 将操作系统置备为裸机设备

引导至仅支持 DASH 的电源状态

启用 DASH 的设备比 vPro 设备支持更多电源状态。可以在 HPCA Console 中执行以下电源操作以将 DASH 设备引导至这些状态之一：

- 挂起
- 休眠 （软）
- 关闭 （有序软关机）
- 关闭 （有序硬关机）
- 关闭 （硬）
- 循环通电 （有序软通电）
- 循环通电 （有序硬通电）
- 循环通电 （硬）
- 主总线重置 （有序）
- 主总线重置
- 诊断中断

这些操作和它们所映射的电源状态的描述，请参见表 13 （第 84 页）表。

HPCA Console 中将 DASH 设备引导到这些电源状态之一的过程相同。唯一差别在于用以下步骤指定该状态的特定电源操作。

用前述操作之一引导 DASH 设备

1. 登录到 HPCA Console，然后选择**操作**选项卡。
2. 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。
3. 单击要管理的 DASH 设备的主机名链接。将打开一个管理窗口。
4. 在窗口左侧的**诊断**部分下，单击**远程操作**链接。此时将打开 “远程操作向导” 窗口。
5. 单击**下一步**继续。此时将打开 “任务” 窗口。
6. 从**远程操作**旁边的下拉菜单，选择将 DASH 设备引导至所需电源状态的电源操作。

   在 “任务” 窗口中，您也可以从下拉菜单选择**显示客户端控制台**选项，指定是否要在控制台上显示文本。
7. 单击**下一步**。此时将打开 “引导设置” 窗口。在此窗口中，可以指定在引导设备时要使用的引导源或引导配置。有关详细信息，请参见配置 vPro 设备上的引导设置 （第 108 页）。对于电源关闭和休眠操作，此步骤无关。
8. 单击**下一步**。此时将打开 “确认摘要” 窗口。在此窗口中检查信息。
9. 单击**下一步**继续。管理控制台上将显示摘要信息。
10. 单击**关闭**。

可以使用此功能将 DASH 设备引导至各种电源状态级别。

vPro 设备上的 KVM 重定向

工作区的**诊断**区域允许您使用键盘视频鼠标重定向 (KVM) 技术，以文本和图形模式访问 vPro 设备的远程控制台。

KVM 正确工作的要求如下：

- vPro 设备必须具有 AMT 6.0 或更高版本。
- JRE 1.6.x 和 VNC Viewer 必须安装在运行浏览器的计算机上，以便访问 HPCA Console。VNC 查看器使用端口 5900。
- 在访问 HPCA Console 的计算机上，必须将 **VNC_PATH** 环境变量设置为安装 VNC Viewer 的路径。例如：**VNC_PATH=C:\viewer\VNCViewer.exe**。
- 必须有 vPro Web 服务的管理权限。若要获得这些权限，在 Intel AMT 控制台中创建 SCS 配置文件时，必须选择 **PT Administration** 领域。

在 vPro 设备上执行 KVM 重定向

1. 登录到 HPCA Console，然后选择**操作**选项卡。
2. 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。
3. 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。
4. 在窗口左侧的**诊断**下单击 **KVM 重定向**链接。此时将打开 “KVM 重定向设置” 窗口。
5. 在 KVM 会话部分的设置中，指定以下内容：
   - 创建并确认 VNC 会话的密码。这是一次性密码，为确保安全，必须对每个新 VNC 会话重置此密码。
   - 在访问用户计算机之前，如果要从该用户获取显式权限，请选中**启用 Opt-in** 选项旁边的框。这提供需要密码验证的第二个级别的更大安全性。

     ➤ 仅当在客户端 vPro 设备上启用选项时，才可能在 HPCA Console 中启用此选项。若要在 vPro 设备上启用选项，请转到客户端 vPro 设备的 MEBx 控制台中。选择 **Main Menu** > **Intel ® AMT Configuration** > **KVM Configuration** > **Opt-in Configurable from remote IT** > **Enable Remote Control of KVM Opt-In Policy**。

     此选项在默认情况下是启用的。
6. 单击**提交**。 VNC Viewer 打开，提示您输入密码。
7. 键入 “KVM 重定向密码” 窗口中创建的会话密码以进行验证。
8. 单击**确定**。

如果已经启用 opt-in 选项，则 AMT KVM opt-in 窗口会打开，提示您输入第二个密码。从要访问的 vPro 设备的用户获取此密码。在用户的 vPro 设备上， KVM 远程协助弹出窗口出现（启用 opt-in 时），其中显示用户同意代码。必须从用户处获取此用户同意代码，将它输入 AMT KVM opt-in 窗口中，然后单击**是**。

vPro 设备的远程控制台打开。

管理 vPro 设备上的系统防御过滤器

工作区的**系统防御**区域仅对 vPro 设备可用。它允许您管理单个 vPro 设备的系统防御过滤器。可以查看和移除已部署到特定 vPro 设备的系统防御过滤器。系统防御过滤器将分配到系统防御策略。分配到策略的过滤器在其相应策略成为活动策略时激活。

打开系统防御过滤器管理窗口

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**系统防御**部分下，单击**过滤器**链接。将打开窗口，显示已通过 HPCA Console 创建并部署到 vPro 设备的系统防御过滤器。

刷新系统防御过滤器视图

1 如打开系统防御过滤器管理窗口中所述打开系统防御过滤器的管理窗口。

2 单击工具栏上的 刷新图标。

查看系统防御过滤器详细信息

1 如打开系统防御过滤器管理窗口中所述打开系统防御过滤器的管理窗口。

2 单击您要查看其详细信息的系统防御过滤器的名称链接。将打开“网络过滤器详细信息”窗口，显示过滤器的规范。

移除系统防御过滤器

1 如打开系统防御过滤器管理窗口中所述打开系统防御过滤器的管理窗口。

2 选中要删除的每个过滤器旁边的框。

3 单击 删除图标。所选过滤器将从 vPro 设备的 “系统防御过滤器” 表中移除。

您可以使用系统防御过滤器界面：

- 查看可以应用于已部署到 vPro 设备的策略的现有过滤器集。
- 移除 vPro 设备上不再需要的过滤器。

管理 vPro 设备上的系统防御策略

工作区的**系统防御**区域仅对 vPro 设备可用。它允许您查看、移除和启用已部署到特定 vPro 设备的系统防御策略。根据优先级，已启用策略变为活动的时，与此策略关联的过滤器将激活

打开系统防御策略管理窗口

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**系统防御**部分下，单击**策略**链接。将打开窗口，显示已通过 HPCA Console 创建并部署到 vPro 设备的系统防御策略。

刷新系统防御策略视图

1 如打开系统防御策略管理窗口中所述，打开系统防御策略管理窗口。

2 单击工具栏上的 刷新图标。

在部署到有线和无线 NIC 的策略之间切换

仅当 vPro 设备同时具有有线和无线网络接口卡 (NIC) 时，此过程才适用。

1 如打开系统防御策略管理窗口中所述，打开系统防御策略管理窗口。如果设备具有 2 个 NIC，则将打开一个窗口，显示已在 vPro 设备上创建并部署到有线 NIC 的系统防御策略。

2 单击 无线图标 （仅当 vPro 设备上同时具有有线和无线 NIC 时，才出现此图标）。将打开窗口，显示创建并部署到 vPro 设备的无线 NIC 上的系统防御策略。

3 单击 有线图标可切换到显示部署到 vPro 设备上有线 NIC 的系统防御策略的窗口。

查看系统防御策略详细信息

1 如打开系统防御策略管理窗口中所述，打开系统防御策略管理窗口。

2 单击您要查看其详细信息的系统防御策略的名称链接。将打开 “系统防御策略详细信息” 窗口，显示策略的规范。

3 单击**下一步**查看与策略关联的过滤器。

4 如果在 vPro 设备上有多个 NIC，则如在部署到有线和无线 NIC 的策略之间切换（第 103 页）中所述单击切换图标，对其他 NIC 重复此过程。

设置代理程序存在策略

1 如打开系统防御策略管理窗口（第 103 页）中所述，打开系统防御策略管理窗口。

2 选中要设为由监视程序操作启用的代理程序存在策略的策略旁边的框。只能选择一个策略作为代理程序存在策略。

3 单击工具栏上的 设置图标。所选策略成为代理程序存在策略。此策略可以通过监视程序操作来启用。如果它比已启用的系统防御策略有更高优先级，则它将成为活动策略。

4 如果在 vPro 设备上有多个 NIC，则如在部署到有线和无线 NIC 的策略之间切换（第 103 页）中所述单击切换图标，对其他 NIC 重复此过程。

启用系统防御策略

1 如打开系统防御策略管理窗口（第 103 页）中所述，打开系统防御策略管理。

2 选中要启用的策略旁边的框。只能选择一个策略。

3 单击工具栏上的 启用图标。所选策略成为新的系统防御默认策略。

4 如果在 vPro 设备上有多个 NIC，则如在部署到有线和无线 NIC 的策略之间切换（第 103 页）中所述单击切换图标，对其他 NIC 重复此过程。

移除系统防御策略

1 如打开系统防御策略管理窗口（第 103 页）中所述，打开系统防御策略管理窗口。

2 选中要删除的每个策略旁的框。

3 单击工具栏上的 删除图标。将从特定 vPro 设备的系统防御策略表移除所选策略。

4 如果在 vPro 设备上有多个 NIC，则如在部署到有线和无线 NIC 的策略之间切换（第 103 页）中所述单击切换图标，对其他 NIC 重复此过程。

您可以使用系统防御策略界面：

- 在 vPro 设备上查看系统防御策略。
- 启用可根据优先级成为活动策略的系统防御策略。
- 将策略设置为可通过监视程序操作启用的代理程序存在策略。如果此策略有更高优先级，它将成为活动策略。
- 移除不再需要的策略。

管理 vPro 设备上的启发

工作区的**系统防御**区域仅对 vPro 设备可用。它允许您查看和移除已部署到特定 vPro 设备的启发信息。

打开启发管理窗口

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**系统防御**部分下，单击**启发**链接。将打开窗口，显示已通过 HPCA Console 创建并部署到 vPro 设备的启发。

刷新启发视图

1 如打开启发管理窗口中所述打开启发管理窗口。

2 单击工具栏上的 刷新图标

查看启发规范详细信息

1 如打开启发管理窗口中所述打开启发管理窗口。

2 单击要查看其详细信息的启发的名称链接。将打开 “启发详细信息” 窗口，显示启发的规范。

3 单击**关闭**以关闭详细信息窗口。

查看设备上 NIC 接口的启发状态信息

1 如打开启发管理窗口中所述打开启发管理窗口。

2 单击您要查看其 NIC 接口状态信息的启发的 NIC 类型链接。“启发状态信息” 窗口打开 , 显示特定 NIC 接口的状态信息。它将指示是否满足启发条件以及已采取的操作。

3 单击**关闭**以关闭状态信息窗口。

清除启发操作

1 如打开启发管理窗口中所述打开启发管理窗口。

2 选中要清除相关操作的每个启发旁的框。

3 单击工具栏上的 清除启发操作图标。将清除与所选启发关联的操作。因此，将不再阻止出站包，打开怀疑的端口，并停用指定的系统防御策略。

移除启发

1 如打开启发管理窗口 （第 105 页）中所述打开启发管理窗口。

2 选中要删除的每个启发旁的框。

3 单击工具栏上的 删除图标。将从特定 vPro 设备的启发表移除所选启发。

使用 “启发” 界面可以：

- 查看 vPro 设备上的启发。
- 移除不再需要的启发信息。

管理 vPro 设备上的监视程序

工作区的**系统防御**区域仅对 vPro 设备可用。它允许您查看和移除已部署到特定 vPro 设备的监视程序。

打开监视程序管理窗口

1 登录到 HPCA Console，然后选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**系统防御**部分下，单击**监视程序**链接。将打开窗口，显示已通过 HPCA Console 创建并部署到 vPro 设备的监视程序。

刷新监视程序视图

1 如打开监视程序管理窗口中所述打开监视程序管理窗口。

2 单击工具栏上的 刷新图标。

查看监视程序详细信息

1 如打开监视程序管理窗口中所述打开监视程序管理窗口。

2 单击要查看其详细信息的监视程序的名称链接。将打开 “监视程序详细信息” 窗口，显示监视程序的规范。

3 单击**关闭**以关闭详细信息窗口。

移除监视程序

1 如打开监视程序管理窗口中所述打开监视程序管理窗口。

2 选中要删除的每个监视程序旁的复选框。

3 单击工具栏上的 删除图标。将从特定 vPro 设备的监视程序表移除所选监视程序。

使用 “监视程序” 界面可以：

- 查看 vPro 设备上的代理监视程序。
- 移除不再需要的监视程序。

配置 vPro 设备上的前面板设置

工作区的**常规设置**区域仅对 vPro 设备可用。它允许您在远程电源操作期间在 vPro 设备上锁定和解锁键盘及电源按钮。

用户可以根据目标设备的功能设置前面板设置。前面板的设置功能取决于特定 vPro 设备的 BIOS。如果设备的 BIOS 不支持前面板设置，则无法从 HPCA Console 控制该功能。建议您与硬件供应商核实与特定支持相关的信息。

配置前面板设置

1 登录到 HPCA Console，并选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**常规设置**部分下，单击**前面板设置**链接。此时打开 “前面板设置” 对话框。

5 单击**此处**链接，以启用对话框的**前面板设置**部分。如果设备支持前面板设置，则将默认锁定设置设为**是**。

6 如果希望 vPro 设备上的键盘和 / 或电源按钮在远程电源操作期间锁定，请保留默认设置。

7 单击**更新**。屏幕上将显示确认消息。

8 单击**关闭**退出该对话框。

可以使用前面板设置，确保从 HPCA Console 执行远程电源操作时没有本地干扰。

重置 vPro 设备上的闪存限制

工作区的**常规设置**区域仅对 vPro 设备可用。它允许您为 vPro 设备重置闪存限制。有关闪存的详细信息，请参见常见实用程序的管理 （第 78 页）。

重置闪存限制

1 登录到 HPCA Console，并选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

3 单击要管理的 vPro 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**常规设置**部分下，单击**闪存限制重置**链接。“闪存限制重置”对话框打开。

5 单击**重置**。显示确认消息。

6 单击**确定**继续。设备上的 3PDS 内存的计数器重置为零。

您可以使用闪存限制重置来重置 vPro 设备上的 3PDS 计数器，后者充当闪存损耗保护机制。此功能允许您继续执行写入到此非易失性存储器的活动。

配置 vPro 设备上的引导设置

工作区的**配置设置**区域仅对 DASH 设备可用。DASH 设备可以具有多个引导配置设置。您可以选择任何一个可用的引导配置设置在引导过程中使用。

每个引导配置设置都可以附加任意数量的可用引导源，例如，硬盘驱动器、CD、USB 等等。而且，每个引导配置设置对附加的引导源都可以有自己的引导顺序。同一引导源可以附加到多个引导配置设置。

工作区的这一区域允许您查看可用的引导配置设置，配置一次性引导配置，以及更改在 DASH 设备上远程操作时的引导顺序。有关详细信息，请参见更改电源状态 （第 90 页）。

配置引导设置

1 登录到 HPCA Console，并选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**设备管理**。将打开 “设备管理”窗口。

3 单击要管理的 DASH 设备的主机名链接。将打开一个管理窗口。

4 在窗口左侧的**配置设置**部分下，单击**引导配置**链接。显示引导配置列表。

➤ 目前，对于 Broadcom DASH 设备，只有两个引导配置设置可用，即**引导配置设置 1** 和**引导配置设置 2**。

该列表指出有关引导配置设置的以下内容：

— **默认**：如果选中，它是计算机系统制造商标记为其默认引导配置的引导配置设置。**默认**设置*不*影响在引导过程中要应用的引导配置。

— **下一次**：如果选中，它是下次引导 DASH 设备 （和后续重新启动）使用的引导配置设置，除非选择**仅下一次**。

➤ 如果是当前的 Broadcom DASH 设备，**引导配置设置 1** 始终是**下一次**的引导配置设置，它无法更改。

— **仅下一次**：如果选中，它是 DASH 设备下次引导期间使用的引导配置设置，之后将不再使用。**仅下一次**引导配置设置优先于**下一次**引导配置设置。

— **当前**：如果选中，它是上次成功引导 DASH 设备所用的引导配置设置。

➤ 当前您只会在**下一次**列中看到选中标记，选择**一次性引导配置**时，会在**仅下一次**列中看到。

— **引导顺序**：附加到引导配置设置的引导源和顺序。

➤ 如果以绿色文本显示**引导顺序**列中的引导源，则它表示错误状态，说明当前引导过程在使用这些引导源设备。这是硬件的错误。如果看到设备以绿色文本显示，必须按以下步骤中的说明，用引导配置向导更改引导顺序。

5 选择要在 “引导配置” 列表中管理的引导配置设置。

6 从引导配置列表表的工具栏上的 引导配置参数图标上的下拉菜单，选择要执行的引导配置选项。目前只能选择以下选项：

— **一次性引导配置** : 更改下次设备通电或重新启动的引导顺序。这次以后，它将恢复为当前引导配置的引导顺序。

选择此选项时，将打开 “更新引导配置向导”。

7 单击**下一步**继续。此时将打开 “设置” 窗口。

8 在**当前引导顺序**列表中选择引导设备，并单击**添加**将它加入**新引导顺序**列表。要从**新引导顺序**列表删除某引导设备，请选择该设备并单击**删除**。

当前引导顺序列表显示可引导设备的所有引导设备。当前引导顺序目前使用的引导设备会以黑色文本显示。当前引导顺序未使用的可用引导设备会以灰色文本显示。

9 对新的引导顺序满意后，单击**下一步**。将打开 “完成” 窗口，显示状态信息。

10 单击**关闭**退出该向导。您已做的更改将反映在 “引导配置” 列表中。

您可以使用该功能查看和更改 DASH 设备的引导配置设置，作为帮助诊断远程电源管理问题的工具。

6 组管理

本章告诉您如何通过 HPCA Console 管理包含 vPro 设备的 Client Automation 设备组。不管电源状态、操作系统的运行状况如何或是否存在管理代理程序，您都可以远程管理包含 vPro 设备的 Client Automation 组。

HPCA Console 中的**操作**选项卡上的带外管理选项之一是**组管理**。

除非已选择管理 vPro 设备，否则该选项不会存在于 HPCA Console 中。

此选项允许您执行以下操作：

- 管理多个 vPro 设备组
- 管理单个 vPro 设备

管理多个 vPro 设备组

管理组时，可以通过以下操作指定显示的组及其在组列表中的排序方式：

- 根据搜索条件搜索特定组
- 为了更方便地查看，选择一次可显示的组数以只看到组子集
- 根据列标题对组排序

组列表的工具栏上的图标使您可以同时管理多个组。

表 18　组列表工具栏

图标	功能
	刷新列表中显示的组
	将列表中显示的设备组与 Client Automation 储备库同步
	对选择的组执行电源管理任务
	管理所选组的警告订阅
	部署所选组的 OOBM 代理程序软件列表
	置备设备组

表 18　组列表工具栏 （续）

图标	功能
	将系统防御策略部署到所选组或从组取消部署
	将监控程序部署到所选组或从组取消部署
	将启发部署到所选组或从组取消部署

如设备列表工具栏表中所示，图标允许您通过将组列表中显示的组设备信息与当前设备信息同步，来手动重新加载这些信息。除了手动重新加载以外， OOBM 可以按固定时间间隔自动重新加载组列表。此时间间隔可在 `config.properties` 文件 （位于 `<HPCA_Install_DIR>\oobm\conf\` 目录）中配置，方法是将 `group_synchronization_timeperiod` 参数设置为新值。

同步时间间隔的默认值为零，表示不会自动同步。如果希望自动同步，请将新值设为非零值。此值的单位是分钟。

多个组选择

选择多个组

1 登录到 HPCA Console，选择**操作**选项卡。

2 在左导航窗格中的**带外管理**下，单击**组管理**。“组管理”窗口打开，显示所有 Client Automation 组。包含 vPro 设备的组将在表中显示为活动链接，表示它们可以通过控制台管理。

3 通过选择要访问的组的复选框，或选择左上方的 “全选”复选框，选择组。可以基于某些条件搜索组，并将组排序以方便选择。

同步组列表与 Client Automation 储备库

同步组列表与 Client Automation 储备库

- 要立即从 Client Automation 储备库重新加载组列表，请从 重新加载图标的下拉菜单选择**立即重新加载组**。选择此选项时，会立即执行重新加载，并且在处理时，会在组列表窗口中看到活动。处理完成时，组列表将显示 Client Automation 储备库中当前找到的组。

- 要以后台进程的形式立即从 Client Automation 储备库重新加载组列表，请从 重新加载图标的下拉菜单选择**后台重新加载组**。选择此选项时，不会在组列表窗口中看到活动。可以通过选择 重新加载图标的下拉菜单的**查看重新加载状态**检查此后台进程的状态。处理完成时，必须单击 刷新图标才能看到重新加载的组列表。

电源管理

设备组电源管理

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 在工具栏上单击 电源管理图标。此时将打开 “电源操作向导”。

3 单击**下一步**。此时将打开 “选项”窗口。

4 选择要在所选组上执行的电源操作。

5 单击**下一步**。此时将打开 “摘要”窗口。

6 单击**下一步**。此时将打开 “完成”窗口，显示操作结果。

7 单击**关闭**退出该向导。

可以使用此功能在特定时间有效地打开和关闭多个设备组，以节约成本。

警告订阅管理

管理设备组上的警告订阅

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 单击 警告订阅管理图标。此时将打开 “警告订阅管理向导”。

3 单击**下一步**。此时将打开 “选项”窗口。

4 选择要订阅还是取消订阅警告。

5 单击**下一步**。此时将打开 “摘要”窗口。

6 单击**下一步**。此时将打开 “完成”窗口，显示操作结果。

7 单击**关闭**退出该向导。

您可以使用此功能对多个设备组执行订阅和取消订阅，这样有关事件的警告就可以发送到 HPCA Console。

OOBM 代理程序软件列表的部署

部署 OOBM 代理程序软件列表

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 单击 部署软件列表图标。此时将打开 “软件部署向导”。

3 单击**下一步**。此时将打开 “软件”窗口。

4 选择要添加到软件列表以部署到所选组的软件名称。

5 单击**下一步**。此时将打开 “摘要” 窗口。

6 单击**下一步**。此时将打开 “完成” 窗口，显示操作结果。

7 单击**关闭**退出该向导。

可以使用此功能创建软件应用程序主列表，以从中选择要 OOBM 代理程序在目标 vPro 设备组上监视的应用程序自定义列表。

置备

执行置备操作

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从 置备图标上的下拉菜单选择**执行置备操作**。此时将打开 “置备操作向导”。

3 单击**下一步**。此时将打开 “选项” 窗口。

4 选择要在所选组上执行的置备操作。置备操作的说明请参见执行置备任务 （第 69 页）。

5 单击**下一步**。此时将打开 “摘要” 窗口。

6 单击**下一步**。此时将打开 “完成” 窗口，显示操作结果。

7 单击**关闭**退出该向导。

查看置备状态日志

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从置备图标上的下拉菜单选择**查看置备状态日志**。此时将打开 “置备状态日志” 窗口。置备操作的状态显示在日志中。

可以使用此功能轻松有效地在设备组上执行置备操作并查看结果。

系统防御策略的部署

部署系统防御策略

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从 管理系统防御策略图标的下拉菜单选择**部署系统防御策略**。此时将打开“策略部署向导”。

3 单击**下一步**。此时将打开 “策略” 窗口。

4 选择要部署到所选组的系统防御策略。

5 单击**下一步**。此时将打开 “设置” 窗口。

6 从下拉菜单选择要在设备组上分配给有线和无线网卡的 “代理程序存在” 和 “系统防御” 策略。

7 单击**下一步**。此时将打开 “摘要” 窗口。

8 单击**下一步**。此时将打开 “完成” 窗口，显示操作结果。

9 单击**关闭**退出该向导。

取消部署系统防御策略

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从 管理系统防御策略图标的下拉菜单选择**取消部署系统防御策略**。此时将打开 “取消策略部署向导”。

3 单击**下一步**。此时将打开 “策略” 窗口。

4 选择要从所选组取消部署的策略。

5 单击**下一步**。此时将打开 “摘要” 窗口。

6 单击**下一步**。此时将打开 “完成” 窗口，显示操作结果。

7 单击**关闭**退出该向导。

可以使用此功能方便地将多个系统防御策略部署至多个 vPro 设备组，以保护这些系统免受恶意攻击。

监视程序的部署

部署监视程序

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从 管理监视程序图标的下拉菜单选择**部署监视程序**。此时将打开 “监视程序部署向导”。

3 单击**下一步**。此时将打开 “监视程序” 窗口。

4 选择要部署到所选组的监视程序。

5 单击**下一步**。此时将打开 “摘要” 窗口。

6 单击**下一步**。此时将打开 “完成” 窗口，显示操作结果。

7 单击**关闭**退出该向导。

取消部署监视程序

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从 管理监视程序图标的下拉菜单选择**取消部署监视程序**。此时将打开 “监视程序取消部署向导”。

3 单击**下一步**。此时将打开 “监视程序” 窗口。

4 选择要从所选组取消部署的监视程序。

5 单击**下一步**。此时将打开 “摘要”窗口。

6 单击**下一步**。此时将打开 “完成”窗口，显示操作结果。

7 单击**关闭**退出该向导。

可以使用此功能方便地将多个监视程序部署至多个 vPro 设备组，以便在这些系统上监视 OOBM 代理程序。监视 OOBM 代理程序增强了网络的安全性，因为这些代理程序会反过来监视已置备设备上运行的安全软件。如果安全软件停止运行 （无意或有意地用户干预），则监视程序可以警告此事件的系统管理员。

启发的部署

部署启发

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从 管理启发图标的下拉菜单选择**部署启发**。此时将打开 “启发部署向导”。

3 单击**下一步**。此时将打开 “启发”窗口。

4 选择要部署到所选组的启发。

5 单击**下一步**。此时将打开 “设置”窗口。

6 从下拉菜单选择要在设备组上分配给有线和无线网卡的启发。

7 单击**下一步**。此时将打开 “摘要”窗口。

8 单击**下一步**。此时将打开 “完成”窗口，显示操作结果。

9 单击**关闭**退出该向导。

取消部署启发

1 如选择多个组 （第 112 页）中所述，选择要管理的组。

2 从 管理启发图标的下拉菜单选择**取消部署启发**。此时将打开 “启发取消部署向导”。

3 单击**下一步**。此时将打开 “启发”窗口。

4 选择要从所选组取消部署的启发。

5 单击**下一步**。此时将打开 “摘要”窗口。

6 单击**下一步**。此时将打开 “完成”窗口，显示操作结果。

7 单击**关闭**退出该向导。

可用此功能将多个启发部署至多个 vPro 设备组，以控制受感染设备的蠕虫病毒。

管理单个 vPro 设备

在**组管理**窗口上显示的组列表中，显示了组类型、组中的设备数、其创建日期和其他属性。

要下溯，以管理组中的单个设备，请单击表的 “描述” 列下的组名称链接。此时将打开 “组详细信息” 窗口。此窗口有以下带选项卡的部分：

- “常规” 选项卡
- “属性” 选项卡
- “设备” 选项卡

“常规” 选项卡

常规选项卡上有 “常见任务” 和 “摘要” 区域。“常见任务” 区提供的链接可用作其他选项卡部分所提供功能的快捷方式。“摘要” 区域提供有关设备组的统计信息。

“属性” 选项卡

属性选项卡显示所选组的属性。为更好了解组属性，请参见 《HP Client Automation Core 和 Satellite Standard Edition 用户指南》 (HP Client Automation Core and Satellite Standard Edition User Guide)。

“设备” 选项卡

设备选项卡显示属于所选组的 vPro 设备的列表。可以管理组中的多个或单个设备。有关详细信息，请参见第 5 章，设备管理。

7 警告通知

本章提供有关查看 vPro 设备上的警告的信息。

查看 vPro 设备上的警告

您可以使用 HPCA Console 查看事件警告。这些警告由置备的 vPro 设备在发生事件时生成，并将发送到 HPCA Console。如果设备订阅了警告，您将看见警告。

刷新警告视图

1 登录到 HPCA Console，并选择**操作**选项卡。

2 在**带外管理**下，单击**警告通知**。此时将打开 “警告通知” 窗口。此选项卡显示 vPro 设备 （已为其订阅警告）生成的警告。

3 单击工具栏上的 刷新图标。

查看有关 vPro 警告的详细信息

1 登录到 HPCA Console，并选择**操作**选项卡。

2 在**带外管理**下，单击**警告通知**。“警告通知” 窗口将打开。此选项卡显示 vPro 设备 （已为其订阅警告）生成的警告。

3 单击 “详细信息” 列中的 详细信息图标。将打开一个窗口，显示所选警告的属性详细信息。

您可以使用警告订阅来确定是否出现了值得注意的事件警告，需要立即采取操作。

8 用例方案

本章解释了如何在管理 OOB 设备时使用 HPCA Console 执行一些标准方案。这些方案考虑到如何可以发现设备资产，执行各种修复功能，以及保护网络上的 vPro 设备免受恶意程序攻击。使用 HPCA Console，不管设备电源状态、操作系统状况如何或是否存在管理代理程序，都可以对设备进行远程管理。这些方案不是 HPCA Console Out of Band Management (OOBM) 功能将来在您企业中的应用的完整详尽表述，而是一些举例说明。

本节介绍以下用例：

- 硬件故障和更换
- 操作系统故障和重新引导
- 病毒感染检测和隔离
- 设备隔离和修复
- 监视关键软件
- 蠕虫病毒感染和控制

➤ 这里介绍的大多数用例都与 vPro 设备有关。如涉及 DASH 设备，则会特别指出。但是，DASH 设备的导航和过程详细信息可能会有所不同。有关详细的过程信息，请参见第 5 章，设备管理。

硬件故障和更换

下面各节分别对此用例进行了介绍：

- 概述
- 用例步骤

概述

发生硬件传感器类型故障。故障导致驻留在 vPro 芯片上的事件管理器引发了事件。根据事件过滤器中的信息，事件管理器将事件警告发送给 HPCA Console。

管理员想要

- 订阅 vPro 设备的事件警告通知 （订阅必须在硬件发生故障前生效）。
- 发现 vPro 或 DASH 设备上的硬件资产以获取正确的更换部件。

订阅 vPro 设备的警告通知后，事件警告便会自动发送到 HPCA Console。这样，管理员就可查找该设备的硬件库存，订购正确的更换部件以使计算机能够再次正常运行。

用例步骤

订阅 vPro 设备的事件警告通知

1 在左侧导航菜单的**操作**选项卡的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

2 通过选中要订阅的设备的复选框，或选中左上方的 “全选” 复选框，来选择设备。

3 从 警告订阅管理图标下拉列表中，选择**订阅警告**。

有关详细信息，请参见警告订阅管理 （第 78 页）。

查看警告

1 在左侧导航菜单的**操作**选项卡的**带外管理**下，单击**警告通知**。此时将打开 “警告通知” 窗口。

2 查看已发送给 HPCA Console 的感兴趣的警告。在本用例中，您要专门查看硬件故障所引发的事件警告。

有关详细信息，请参见查看 vPro 设备上的警告 （第 119 页）。

查看硬件资产

1 在左侧导航菜单的**操作**选项卡的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

2 单击存在硬件故障的 vPro 设备的主机名链接。

3 在窗口左侧**诊断**下方的表中，单击 “设备” 列的**设备资产**链接。

4 单击**硬件信息**。

5 单击有故障的硬件组件。该组件的规格即会显示在控制台内容区域。

有关详细信息，请参见查看硬件资产 （第 88 页）。

然后，您可以根据通过 HPCA Console 从 vPro 或 DASH 设备处获得的信息来订购更换部件。

操作系统故障和重新引导

下面各节分别对此用例进行了介绍：

- 概述
- 用例步骤

概述

vPro 或 DASH 设备上的操作系统没有响应。计算机用户将这一情况通知了管理员。

管理员想要

- 锁定远程 vPro 设备前面板 （在此示例中，假定 vPro 设备支持该功能），这样执行远程电源操作时便不会有用户干涉。前面板设置功能在 DASH 设备上不可用。
- 从 HPCA Console 服务器上的操作系统映像文件重新启动计算机，以进一步诊断问题。

用例步骤

锁定 vPro 设备前面板

1 在左侧导航菜单的**操作**选项卡的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

2 在 “设备” 列中，单击有操作系统故障的 OOB 设备的主机名链接。

3 在窗口左侧**常规设置**下，单击**前面板设置**链接。

4 单击**此处**链接，以启用对话框的**前面板设置**部分。

5 确保键盘和电源按钮的设置已设为**是**。

有关详细信息，请参见配置 vPro 设备上的前面板设置 （第 107 页）。

用 IDE-R CD 驱动器重新启动系统

1 在左侧导航菜单的**操作**选项卡的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

2 单击有操作系统故障的 vPro 设备的主机名链接。

3 在窗口左侧**诊断**下，单击**远程操作**链接。

4 在远程操作向导中，为 “远程操作” 选择**重新启动到 IDE-R**，并为应用前面板设置选项选择**是**。

5 在 “驱动器路径” 字段，输入 ISO 文件在管理控制台服务器上的路径。

6 执行向导中的其余步骤。

有关详细信息，请参见重新启动带 IDE-R 的 vPro 系统 （第 95 页）。

病毒感染检测和隔离

下面各节分别对此用例进行了介绍：

- 概述
- 用例步骤

概述

vPro 设备检测到的网络流量与当前处于活动状态的系统防御策略的速率限制过滤器相匹配，因此怀疑病毒攻击。该匹配导致驻留在 vPro 芯片上的事件管理器引发事件。根据事件过滤器中的信息，事件管理器将事件警告发送给 HPCA Console。

管理员想要：

- 订阅 vPro 设备的事件警告通知。
- 创建与所需过滤器关联的隔离策略，以便病毒限制在受感染的设备上，而不会传染给网络上的其他设备。
- 启用、激活并部署策略到受感染的 vPro 设备。
- 修复、更换或拆除设备。
- 设备安全时禁用策略。

创建、部署并激活策略后，vPro 设备会检查数据包，并执行由与隔离策略关联的过滤器所指定的操作。在这种情况下，过滤器会丢弃所有由此设备传输的 TCP 数据包。一旦计算机与网络设备隔离，管理员就可执行还原 vPro 设备所需的修复任务，然后禁用隔离策略。

用例步骤

订阅 vPro 设备的事件警告通知

按用例硬件故障和更换的订阅 vPro 设备的事件警告通知 （第 122 页）中的步骤进行操作。

查看警告

按用例硬件故障和更换的查看警告（第 122 页）中的步骤进行操作。在本用例中，您要专门查看速率限制过滤器所触发的事件警告。

创建隔离过滤器

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**过滤器**。此时将打开 “过滤器” 窗口。

2 单击工具栏上的 添加图标。此时将打开 “系统防御过滤器向导”。

3 单击**下一步**继续。此时将打开 “过滤器详细信息” 窗口。在此窗口中，指定以下信息：

   — **过滤器名称**：输入**隔离**。

   — **过滤器类型**：选择**丢弃**。

   — **与过滤器匹配时创建事件**：选择**是**。

4 单击**下一步**。此时将打开 “参数” 窗口。在此窗口中，指定以下信息：

   — **数据包类型**：选择 **TCP**。

   — **过滤器模式或方向**：选择**传输**。

   — **网络地址**：选择**过滤发往网络的数据包**。

— **端口范围**：选择**源端口范围**。在**最小端口**和**最大端口**值中，输入 **1** 和 **655535**。它们指的是 vPro 设备上的端口数。为了防止 vPro 设备感染其他设备，需要阻止从 vPro 设备上的所有源端口到网络上所有设备的所有目标端口的数据包。

5 单击**下一步**，然后单击**关闭**。

有关详细信息，请参见管理系统防御过滤器 （第 54 页）。

创建隔离策略

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。

2 单击工具栏上的 添加图标。此时将打开 “系统防御策略向导”。

3 单击**下一步**继续。此时将打开 “策略详细信息”窗口。在此窗口中，指定以下信息：

— **策略名称**：输入**隔离**。

— **优先级**：输入 **98**。

— **启用防欺诈过滤器**：选择**是**。

— **默认接收 (Rx) 过滤器类型**：选择**通过**。

— **默认传输 (Tx) 过滤器类型**：选择**通过**。

4 单击**下一步**查看所有可用过滤器。

5 将 “隔离”过滤器拖到**分配给策略的过滤器**列表。

6 单击**添加策略**。

有关详细信息，请参见管理系统防御策略 （第 57 页）。

启用、激活并部署隔离策略到 vPro 设备

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。

2 选中隔离策略旁边的框。

3 单击工具栏上的 部署图标，此时将打开 “策略部署向导”。

4 单击**下一步**继续。此时将打开 “选择设备”窗口。

5 选中受感染的 vPro 设备旁边的框。

6 单击**下一步**。此时将打开 “设置策略”窗口。

7 选择隔离策略作为有线 NIC 的系统防御策略。此操作使隔离策略成为受感染 vPro 设备的系统防御策略。由于创建策略时为此策略指定了最高优先级 (98) （与当前定义的其他系统防御策略有关），它还成为受感染 vPro 设备的活动策略。

8 执行向导中的其余步骤。

有关详细信息，请参见管理系统防御策略 （第 57 页）。

停用 vPro 设备的隔离策略

1 在左侧导航菜单的**操作**选项卡的**带外管理**下，单击**设备管理**。将打开 “设备管理”窗口。

2 单击已感染病毒的 vPro 设备的主机名链接。

3 在窗口左侧的**系统防御**部分下面，单击**策略**链接。此时将打开窗口，显示已部署到此设备的系统防御策略。

4 选中 “隔离” 旁边的框。

5 单击工具栏上的 启用 / 禁用图标。“隔离” 不再是启用的系统防御策略。

有关详细信息，请参见管理 vPro 设备上的系统防御策略 （第 103 页）。

设备隔离和修复

下面各节分别对此用例进行了介绍：

- 概述
- 用例步骤

概述

管理员需要从公司网络中隔离出特定的设备以防止任何攻击。然而，设备需要连接到管理服务器以接收它所需的修复。修复可能包括病毒定义的更新，防火墙软件的新版本，或者管理员对有问题设备的远程控制。

如果阻止了所有网络流量，事实上无法进行设备修复。因此，管理员必须阻止除与修复管理服务器之间的所有网络流量，以便修复受感染的设备。

管理员想要：

- 创建与所需过滤器关联的修复策略，以便除包含修复受感染设备的所需软件的 HP Client Automation 服务器以外，阻止所有网络流量。
- 启用、激活并部署策略到网络上的所有 vPro 设备。
- 修复设备时禁用策略。

创建、部署并激活策略后，vPro 设备会检查数据包，并执行由与修复策略关联的过滤器所指定的操作。在这种情况下，过滤器会通过接收自或传输到 IP 地址与过滤器中的地址匹配的设备的所有 TCP 和 UDP 数据包。在本例中，该地址是 HP Client Automation 服务器的 IP 地址。所有其他数据包将根据策略丢弃数据包的默认操作来丢弃。

用例步骤

您要为修复策略创建 4 个过滤器。您必须完成以下过程 4 次，对于每个需要创建的过滤器执行一次。

创建修复过滤器

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**过滤器**。此时将打开 “过滤器” 窗口。

2 单击工具栏上的 添加图标。此时将打开 “系统防御过滤器向导”。

3 单击**下一步**继续。此时将打开 “过滤器详细信息” 窗口。您要为正在创建的相应过滤器指定以下信息：

表 19 修复过滤器

过滤器名称	过滤器类型	与过滤器匹配时创建事件
PassTCP_Recv	通过	是
PassTCP_Xmit	通过	是
PassUDP_Recv	通过	是
PassUDP_Xmit	通过	是

4 单击**下一步**。此时将打开 “参数” 窗口。您要为正在创建的相应过滤器指定以下信息：

表 20 修复过滤器

过滤器名称	数据包类型	下一个协议	过滤器模式	网络地址
PassTCP_Recv	IP 数据包 (IPv4)	TCP	接收	Device:192.168.5.12
PassTCP_Xmit	IP 数据包 (IPv4)	TCP	传输	Device:192.168.5.12
PassUDP_Recv	IP 数据包 (IPv4)	UDP	接收	Device:192.168.5.12
PassUDP_Xmit	IP 数据包 (IPv4)	UDP	传输	Device:192.168.5.12

5 单击**下一步**，然后单击**关闭**。

您还可以创建这样的过滤器：丢弃除特定子网间 （而非单个设备间）流量之外的所有流量。如果单个子网上驻留了多台修复服务器，则会非常有用。

有关详细信息，请参见管理系统防御过滤器 （第 54 页）。

创建修复策略

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。

2 单击工具栏上的 添加图标。此时将打开 “系统防御策略向导”。

3 单击**下一步**继续。此时将打开 “策略详细信息” 窗口。在此窗口中，指定以下信息：

— **策略名称**：输入**修复**。

— **优先级**：输入 **98**。

— **启用防欺诈过滤器**：选择**是**。

— **默认接收 (Rx) 过滤器类型**：选择**丢弃**。

— **默认传输 (Tx) 过滤器类型**：选择**丢弃**。

4 单击**下一步**查看所有可用过滤器。

5 将 PassTCP_Recv、 PassTCP_Xmit、 PassUDP_Recv 和 PassUDP_Xmit 过滤器拖到**分配给策略的过滤器**列表。

6 单击**添加策略**。

有关详细信息，请参见管理系统防御策略 （第 57 页）。

启用、激活并部署修复策略到 vPro 设备

按用例病毒感染检测和隔离的启用、激活并部署隔离策略到 vPro 设备 （第 125 页）中的步骤进行操作。在本案例中，选择 “修复” 策略。

停用 vPro 设备的修复策略

按用例病毒感染检测和隔离的停用 vPro 设备的隔离策略 （第 125 页）中的步骤进行操作。在本案例中，选择 “修复” 策略。

监视关键软件

下面各节分别对此用例进行了介绍：

- 概述
- 用例步骤

概述

vPro 设备上安装并启动了 OOBM 代理程序，以监视安全软件应用程序列表。受监视的安全应用程序停止时，OOBM 代理程序将停止向监视程序发送检测信号。此转换状态促使监视程序采取管理员在创建监视程序时所指定的操作。在本案例中，监视程序会引发事件，并启用代理程序存在策略。

此类情况通常在用户禁用了防病毒软件时发生，因为他们认为该软件会影响性能。如果防病毒软件没有在运行，安全管理部门希望执行一种策略，将计算机从公司网络中移除。

管理员想要：

- 订阅 vPro 设备的事件警告通知。
- 定义 OOBM 代理程序发生故障时隔离 vPro 设备的系统防御策略，并将此策略设为代理程序存在策略。
- 创建监视程序，并指定其操作。
- 将代理程序存在策略和监视程序部署到 vPro 设备。
- 管理 OOBM 代理程序设置，并将设置部署到 vPro 设备。
- 在 vPro 主机操作系统上安装 OOBM 代理程序 （OOBM 代理程序由安装程序自动启动）。
- 发送事件警告后重新启动安全进程。

在 vPro 设备上安装并启动 OOBM 代理程序后， OOBM 代理程序会向监视程序注册，并以定义的间隔开始向其发送检测信号。一旦代理程序发生故障，代理程序就停止向监视程序发送检测信号。监视程序引发事件，并启用部署的代理程序存在策略。代理程序存在策略根据其较高的优先级成为活动策略。策略激活后，vPro 设备检查数据包，并执行由与代理程序存在策略关联的过滤器所指定的操作。管理员执行修复任务，重新启动 OOBM 代理程序过去所监视的安全软件。安全软件重新启动后，OOBM 代理程序重新注册并开始向监视程序发送检测信号。监视程序禁用代理程序存在策略和启用的系统防御策略，优先级较高的策略将成为下一个活动策略。

用例步骤

查看 vPro 设备的事件过滤器

1 在左侧导航菜单的**操作**选项卡的**带外管理**下，单击**设备管理**。将打开 “设备管理” 窗口。

2 单击要查看事件过滤器的 vPro 设备的主机名链接。

3 在窗口左侧的**诊断**下面，单击**事件过滤器**链接。此时控制台内容区域将显示所选 vPro 设备上存在的默认事件过滤器。

4 单击每个事件过滤器的名称链接，以确定由哪个事件过滤器检测代理程序故障并向管理控制台发送警告。

有关详细信息，请参见查看 vPro 事件过滤器 （第 87 页）。

订阅 vPro 设备的事件警告通知

按用例硬件故障和更换的订阅 vPro 设备的事件警告通知中的步骤进行操作。

为代理程序存在策略创建过滤器

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**过滤器**。此时将打开 “过滤器” 窗口。

2 单击工具栏上的 添加图标。此时将打开 “系统防御过滤器向导”。

3 单击 “下一步” 继续。此时将打开 “过滤器详细信息” 窗口。在此窗口中，指定以下信息：

— **过滤器名称**：输入**阻止感染**。

— **过滤器类型**：选择**丢弃**。

— **与过滤器匹配时创建事件**：选择**是**。

4 单击**下一步**。此时将打开 “参数” 窗口。在此窗口中，指定以下信息：

— **数据包类型**：选择 **TCP**。

— **过滤器模式或方向**：选择**接收**。

— **网络地址**：选择**过滤来自网络的数据包**。

— **端口范围**：选择**目标端口范围**。在**最小端口**和**最大端口**值中，输入 **1** 和 **655535**。它们指的是 vPro 设备上的端口数。为了防止感染 vPro 设备，需要阻止从网络上的所有 vPro 设备的所有源端口到此设备的所有目标端口的数据包。

5 单击**下一步**，然后单击**关闭**。

有关详细信息，请参见管理系统防御过滤器 （第 54 页）。

创建代理程序存在策略

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。

2 单击工具栏上的 添加图标。此时将打开 “系统防御策略向导”。

3 单击 “下一步”继续。此时将打开 “策略详细信息”窗口。在此窗口中，指定以下信息：

— **策略名称**：输入**阻止感染**。

— **优先级**：输入 **99**。

— **启用防欺诈过滤器**：选择**是**。

— **默认接收 (Rx) 过滤器类型**：选择**通过**。

— **默认传输 (Tx) 过滤器类型**：选择**通过**。

4 单击**下一步**查看所有可用过滤器。

5 将 “阻止感染”过滤器拖到**分配给策略的过滤器**列表。

6 单击**添加策略**。

有关详细信息，请参见管理系统防御策略 （第 57 页）。

将代理程序存在策略设置并部署到 vPro 设备

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**策略**。此时将打开“策略”窗口。

2 选中 “阻止感染”策略旁边的框。

3 单击工具栏上的 部署图标，此时将打开 “策略部署向导”。

4 单击**下一步**继续。此时将打开 “选择设备”窗口。

5 选中要运行 OOBM 代理程序的 vPro 设备旁边的框。

6 单击**下一步**。此时将打开 “设置策略”窗口。

7 选择**阻止感染**策略作为有线 NIC 的代理程序存在策略。此操作是将 “阻止感染”策略设为 vPro 设备的代理程序存在策略。如果 OOBM 代理程序停止向监视程序发送检测信号，监视程序将会启用此策略。由于创建策略时指定了最高优先级 (99)，它还将成为活动策略 （如果监视程序启用了该策略）。

8 执行向导中的其余步骤。

有关详细信息，请参见管理系统防御策略 （第 57 页）。

创建监视程序

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开“监视程序”窗口。

2 单击 添加图标创建监视程序。此时将打开 “监视程序向导”。

3 单击**下一步**继续。在此窗口中，指定以下信息：

— **代理程序类型**：选择 **OOBM 代理程序**。

— **名称**：输入 **AlphaWatchdog**。

— **代理程序 GUID**：此字段对于 OOBM 代理程序是灰色的，因为 OOBM 代理程序的 GUID 已知。

— **检测间隔**：接受提供的默认值。

— **启动间隔**：接受提供的默认值。

4 单击**下一步**。此时将打开向导的 “监视程序操作” 页。在此窗口中，指定以下信息：

— **转换状态**：

从：选择**代理程序正在运行**。

到：选择**代理程序已停止**。

— **操作**：

为**代理程序存在**选择**启用**，以指定在发生指定的代理程序转换时启用代理程序存在策略。

为**事件创建**选择**启用**，以指定在发生指定的代理程序转换时引发事件。

5 单击**添加操作**。此时操作便添加到窗口底部的操作表中。

6 再添加一个转换状态的操作。现在，在此窗口中指定以下信息：

— **转换状态**：

从：选择**代理程序已停止**。

到：选择**代理程序正在运行**。

— **操作**：

为**代理程序存在**选择**禁用**，以指定在发生指定的代理程序转换时禁用代理程序存在策略。

为**事件创建**选择**启用**，以指定在发生指定的代理程序转换时引发事件。

7 单击**添加操作**。此时操作便添加到窗口底部的操作表中。

8 执行向导中的其余步骤。

有关详细信息，请参见管理监视程序 （第 64 页）。

将监视程序部署到 vPro 设备

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开“监视程序”窗口。

2 选中 AlphaWatchdog 旁边的复选框。

3 单击工具栏上的 部署监视程序图标。此时将打开 “监视程序部署向导”。

4 单击**下一步**继续。此时将打开 “选择设备” 窗口。

5 选中要运行 OOBM 代理程序的 vPro 设备旁边的复选框。

6 执行向导中的其余步骤。

有关详细信息，请参见管理监视程序 （第 64 页）。

配置系统消息和软件列表

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开“监视程序”窗口。

2 单击 OOBM 代理程序设置图标。此时将打开 “软件列表”对话框。

3 接受**系统消息**文本框中提供的默认消息。

4 在**软件名称**框中，输入 **symantec.exe**。

5 单击**添加**。您可以重复此过程，以创建需要 OOBM 代理程序监视的软件应用程序列表。

6 单击**保存**。此时屏幕上会显示通知消息。

7 单击**关闭**退出该对话框。系统消息和代理程序软件列表将存储在 XML 储备库中。

有关详细信息，请参见配置系统消息和软件列表 （第 68 页）。

部署系统消息和软件列表

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**监视程序**。此时将打开“监视程序”窗口。

2 单击 部署软件列表和系统消息图标。此时将打开 “软件部署向导”。

3 单击**下一步**。此时将打开 “软件标题”窗口。

4 选择 **symantec.exe** 软件应用程序。

5 单击**下一步**。此时将打开 “设备”窗口。

6 选中要运行 OOBM 代理程序的 vPro 设备旁边的复选框。

7 单击**下一步**，然后执行向导中的其余步骤。

有关详细信息，请参见部署系统消息和软件列表 （第 68 页）。

在 vPro 设备上安装并启动 OOBM 代理程序

1 将位于 HPCA Core 分发介质 `Media\oobm\win32\LocalAgent` 目录下的 `oobmclocalagent.msi` 文件复制到 vPro 设备。双击该文件。或者，您还可以将位于分发介质上同一目录下的 `setup.cmd` 文件复制到 vPro 设备。双击安装程序文件，或在命令行输入 `setup.cmd`。 `setup.cmd` 文件会调用 `oobmclocalagent.msi` 文件。

2 单击**下一步**，并接受许可协议。

3 单击**下一步**。此时将打开 “远程配置参数”窗口。在此窗口中，指定以下信息：

— **SCS 配置客户端用户名**：输入具有配置客户端角色的用户的名称。在本例中，它是 **SCSUser@vlan1.hp.com**。

SCS 配置客户端密码：输入 SCSUser 的密码。有关此角色的详细信息，请参见配置客户端角色 （第 26 页）。

— **SCS 配置文件标识**：输入 vPro 设备的配置文件标识。此信息可以在 SCS Console 的 “配置文件” 区域中找到。

— **SCS 远程配置 URL**：输入 URL 路径，包括 Intel 安装和配置服务 (SCS) Web 服务的虚拟目录。在本例中，它是 **https://provisionserver. vlan1.hp.com /amtscs_rcfg**，其中 **provisionserver.vlan1.hp.com** 是 IIS 主机的完全限定域名 (FQDN)， **amtscs_rcfg** 是主机上的 SCS Web 服务虚拟目录。

4 单击**下一步**。此时将打开 “用户信息” 窗口，在其中可以输入 vPro 管理员凭据。在此窗口中，指定以下信息：

— **用户名**：输入 vPro 管理员的用户名。

— **密码**：输入 vPro 管理员的密码。

— 不要选中 **TLS 模式**复选框，因为在本用例中不以 TLS 模式置备 vPro 设备。

5 单击**下一步**，然后执行安装向导中的其余步骤。

有关详细信息，请参见安装 OOBM 代理程序 （第 26 页）。

OOBM 代理程序是 NT 服务，安装后应立即启动。

OOBM 代理程序启动时，OOBM 代理程序要监视的软件列表上的所有应用程序都必须在运行。如果不是，只要 OOBM 代理程序启动就会关闭监视程序。

激活 vPro 设备上的代理程序存在策略

您在创建监视程序时已经为 “正在运行” 到 “已停止” 状态的转换指定了此操作，因此监视程序会自动启用代理程序存在策略。

而且，在创建系统防御策略时将策略设为代理程序存在策略，并将其优先级定义为 99，该策略的优先级比当前活动的系统防御策略高，因此自动成为新的活动策略。

发送警告

您在创建监视程序时已经为 “正在运行” 到 “已停止” 状态的转换指定了此操作，因此监视程序会自动引发事件。

此类事件的默认事件过滤器指定记录事件日志并发送警告，如果订阅了 vPro 设备，事件警告会自动发送到管理控制台。

最后，由于您的确为运行 OOBM 代理程序的 vPro 设备订阅了事件警告通知，事件过滤器现在具有一个已知的警告发送目标，以便它可以将警告发送到管理控制台。

查看警告

按用例硬件故障和更换的查看警告 （第 122 页）中的步骤进行操作。在本用例中，您要专门查看 OOBM 代理程序故障所引发的事件警告。

重新启动安全进程

在命令行输入命令，或双击调用安全应用程序的可执行文件。

停用 vPro 设备上的代理程序存在策略

在 OOBM 代理程序重新开始向监视程序发送检测信号后，监视程序会根据为 “已停止” 到 “正在运行” 状态转换定义的操作，自动禁用代理程序存在策略，已启用的优先级较高的系统防御策略将成为新的活动策略。

蠕虫病毒感染和控制

下面各节分别对此用例进行了介绍：

- 概述
- 用例步骤

概述

尽管网络中有防火墙和入侵检测系统，管理员也知道这些机制仅针对已知的蠕虫病毒，但不能有效阻止零日蠕虫病毒的爆发。要保护网络，避免这样的爆发，则必须使用启发式蠕虫病毒控制系统。

管理员想要：

- 订阅 vPro 设备的事件警告通知。
- 创建启发规范，并定义触发控制操作的阈值 （数据包计数）和窗口大小 （时间）值。
- 指定在以下情况下要采取的操作，即驻留在 vPro 芯片上的启发式规则引擎检测到根据阈值和窗口大小值可能指示蠕虫群袭的网络流量。
- 指定控制操作仍然有效的超时值。
- 将启发规范部署到有漏洞的 vPro 设备。
- 接到可能爆发的警告后，执行所需的修复任务。

当启发信息部署到 vPro 设备后，启发式规则引擎对数据包计数，并更新计数器。如果与启发条件匹配，引擎将触发管理员指定的操作。在本用例中，它将创建事件并阻止有问题端口的出站流量。这一条件的匹配总是导致驻留在 vPro 芯片上的事件管理器引发事件。（在本用例中，假定启用事件警告时 vPro 设备上的事件过滤器有此类事件的条目。）

一旦计算机与网络设备隔离，管理员就可执行还原 vPro 设备所需的修复任务。启发操作在超时值中指定的时间长度内将仍然有效。过了该时间值后，操作会取消，而启发式规则引擎还会继续检查流量。

用例步骤

订阅 vPro 设备的事件警告通知

按用例硬件故障和更换的订阅 vPro 设备的事件警告通知 （第 122 页）中的步骤进行操作。

创建启发规范

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开“启发”窗口。

2 单击 添加图标创建新启发信息。此时将打开 “启发向导”。

3 单击**下一步**继续。此时将打开 “启发详细信息”窗口。在此窗口中，指定以下信息：

- **设置类型：选择默认值。**
- **参数**
  - **名称：**输入 Zero_Worm。
  - **快速数据包计数：**接受默认值 8。
  - **快速时间计数：**接受默认值 10。
  - **慢速数据包计数：**接受默认值 64
  - **慢速时间计数：**接受默认值 50 秒 （50000 毫秒）。
  - **遇到超时：**输入 50 秒。

    有关详细信息，请参见窗口大小和阈值 （第 175 页）和控制操作和超时值 （第 176 页）。
- **操作**
  - **阻止 TX 流量：**从下拉列表中选择**仅有问题端口**。
- **策略**
  - **策略名称：**不要从下拉列表中选择策略名称，因为不需要在符合启发条件时启用系统防御过滤器。

4 单击**下一步**。此时将显示操作状态。

5 单击**关闭**退出该向导。“启发”表中将显示新的启发信息，且该信息已添加到储备库中。

有关详细信息，请参见管理启发信息 （第 61 页）。

部署启发规范

1 在左侧导航菜单的**配置**选项卡的**带外管理 > vPro 系统防御设置**下，单击**启发**。此时将打开“启发”窗口。

2 选中 Zero_Worm 启发规范旁边的框。

3 单击工具栏上的 部署启发图标。此时将打开 “启发向导”。

4 单击**下一步**继续。此时将打开 “选择设备”窗口。

5 选中每个要部署启发信息的设备旁边的框。

6 单击**下一步**。此时将打开 “启发设置”窗口。

7 为所选设备上的有线和无线网络接口都选择 Zero_Worm 启发规范。

8 单击**下一步**。“确认摘要”窗口将打开。在此窗口中检查信息。

9 单击**下一步**继续部署过程。此时将打开 “结果”窗口，显示操作结果。

10 单击**关闭**退出该向导。

有关详细信息，请参见管理启发信息 （第 61 页）。

查看警告

按用例硬件故障和更换的查看警告（第 122 页）中的步骤进行操作。在本用例中，您要专门查看启发式规则引擎所引发的事件警告。

9 疑难解答

本章提供调试信息，可用于调试在 HPCA Console 中使用带外管理功能时发生的最常见问题，如常见问题中所述。

同时说明备份 OOBM 数据以防损坏或需要重新安装产品的最佳做法，如备份 OOBM 数据（第 164 页）中所述。

此外，还概述了带外管理通信的端口要求，如端口信息摘要 （第 165 页）中所述。

并提供了在致电 HP 支持之前需要回答的问题清单，如清单问题 （第 166 页）中所述。

常见问题

通常，在发生问题时，如果是在默认位置中安装 HPCA，查看 < *安装目录* >\tomcat\logs 目录中的日志文件始终是一个好办法。这些文件中包含 HPCA Console 的所有输出。

此外，有关代理程序的问题，可在 vPro 客户端设备上打开事件查看器（**开始 > 设置 > 控制面板 > 管理工具 > 事件查看器**）。

本节中涵盖的疑难解答领域包括：

- 常规
- 置备
- 发现
- 远程操作
- 电源状态
- 重新启动
- 系统防御和代理程序存在
- 无线
- 迁移问题

常规

选择 vPro 设备类型时 HPCA Console 挂起

表 21

可能原因	解决方案
由于 CPU 利用率过高（Tomcat 占用了 100% 的 CPU）， SCS 服务无法与带外管理服务通信。	如果问题依旧存在，请重新启动 HPCA Tomcat 服务器。

替代单个设备控制台显示的错误页面未清除

表 22　错误页面未清除

可能原因	解决方案
Internet Explorer 浏览器缓存未清除。有时替代单个设备控制台显示的错误页面在 Internet Explorer 重新打开之前未清除。	手动清除 Internet Explorer 缓存。

键盘和电源按钮锁定，但是在 HPCA Console 中并未设置为锁定

表 23　前面板锁定问题

可能原因	解决方案
锁定取决于 vPro 设备上运行的 BIOS 的版本。某些版本在默认情况下锁定电源按钮和键盘。	在某些设备上，BIOS 设置可由用户配置。有关可配置的 BIOS 版本，请参见设备文档。

无法使用有线 NIC 连接到 vPro 设备

表 24　vPro 设备上的有线 NIC 连接问题

可能原因	解决方案
可能原因如下： 1　vPro 设备已从网络移除。 2　vPro 设备的 Web 服务繁忙。	在这些情况中，选择需要的设备，并在几秒钟后使用“从储备库刷新”图标刷新 HPCA Console 屏幕，以便可以从 vPro 设备再次获取 HPCA Console Web 服务请求。

使用 HPCA Console 时发生超时

表 25　HPCA Console 超时

可能原因	解决方案
网络流量速度缓慢	重新配置超时期间。有关详细信息，请参见配置 IDE-R 和 SOL 超时值 （第 34 页）。

OOBM 设备管理屏幕上的错误警告订阅状态

表 26　错误警告订阅状态

可能原因	解决方案
由于 OOBM 第三方依赖性而产生的问题。 当 HPCA 安装在 Windows Server 2008 上时，尽管警告订阅操作成功执行，但还是会在状态列中错误报告其状态。这会在用户通过选择**操作** > **带外管理** > **设备管理** > **警告订阅**在 vPro 设备上执行警告订阅操作时引发问题。	没有此问题的解决方法。

在控制台上访问 “OOBM 设备详细信息”窗口时长时间空闲后导致退出到登录屏幕

表 27　长时间空闲期导致退出到登录屏幕

可能原因	解决方案
数据库访问相关问题	关闭浏览器，并在新浏览器会话中重新登录到 HPCA Console。

在设备类型选择窗口中管理 vPro 设备时，无法保存 SCS 属性

表 28　域名通过 SCS 登录验证

可能原因	解决方案
在 SCS 登录中，未以 domainName\userName 格式指定用户名。此格式目前必需并要验证。在 OOBM 的更早版本中，忽略登录名的 domainName 部分。因此，即使提供了错误的 domainName，似乎仍被接受。此外，在更早的 OOBM 版本中，提供的用户名登录 (provisionserver.yourenterprise.com\Administrator) 示例不正确但可用，因为 OOBM 忽略域名。	必须提供正确的 domainName\userName 格式登录用户名，以便保存 SCS 属性。

在更改 DASH 凭据之后，无法访问 DASH 设备

表 29　更改 DASH 凭据时出现问题

可能原因	解决方案
缓存的上一个凭据导致错误行为	如果更改了 DASH 设备凭据，则必须重新启动 Tomcat 服务使其生效。

将 vPro 设备与 SCS 储备库同步花费很长时间

表 30　vPro SCS 同步问题

可能原因	解决方案
执行了多次 Web 服务调用来确定可用 vPro 设备列表。这可能需要几分钟时间，具体取决有多少系统不可用或当前网络上的路由问题。	降低 Web 服务超时值可以提高性能。但是，降低超时值可能导致错过某些可用计算机或无法完成其他操作 （比如电源或部署）。

无法访问正确 vPro 设备

表 31　vPro 访问问题

可能原因	解决方案
IP 地址冲突问题，即多个 vPro 设备可能具有相同 IP 地址	IP 地址必须各不相同。请与网络管理员联系以解决此问题。

在 SQL 操作期间 HyperTerminal 无法正确显示文本

表 32　HyperTerminal 文本显示问题

可能原因	解决方案
HyperTerminal 中可能启用了 “超过终端宽度的行换行” 选项。	打开 HyperTerminal。转到 “文件属性” 。选择**设置**选项卡。单击 **ASCII 设置**。在 “ASCII 安装程序” 窗口中，取消选中 “超过终端宽度的行换行” 选项。

对 OOB 设备软件列表的部署引发 TLS 模式中的网络错误 26

表 33　对软件列表的部署引发 TLS 模式中的网络错误

可能原因	解决方案
客户端证书未在 HP Client Automation 安装计算机上正确配置。 对 OOB 设备软件列表的部署导致在 TLS 模式中引发网络错误 26。这会在用户通过选择**操作** > **带外管理** > **设备管理** > **软件列表部署**执行软件列表部署操作时引发问题。	在 HP Client Automation 安装计算机上安装客户端证书，并指定证书的主题名称作为 `config.properties` 文件中 “ca_server_commonname” 属性的值。

无法读取或写入被管 vPro 设备

表 34　闪存限制异常错误

可能原因	解决方案
超出 vPro 存储的闪存限制。 如果对同一 vPro 设备进行多次读 / 写访问，闪存损耗保护机制会导致闪存限制异常发生。当计数器达到 200 时， vPro 设备不再允许写入操作。	使用 常用实用程序图标的下拉菜单中的**重置闪存限制**选项。有关详细信息，请参见常见实用程序的管理 （第 78 页）。

OOBM 和 SCS 的 I18N 问题

表 35　SCS 的 I18N 问题

可能原因	解决方案
基础组件和技术 （如硬件 BIOS 或 Intel SCS）的依赖性。 尽管 HPCA 控制台可以安装在非英语操作系统上，但有若干限制，这是由于基础组件和技术（如硬件 BIOS 或 Intel SCS）之间的依赖性。因此，不能通过选择**配置 > 带外管理 > vPro 系统防御设置**为几个用户定义项 （包括过滤器、监视程序和策略）输入非英语名称。BIOS 设置的 SOL 控制台仅对支持的字符集有效。类似地，其他功能可能也不会在非英语区域中正常工作。数字、日期和时间都不会以非英语操作系统的区域格式显示。	没有此问题的解决方法。

英语路径分隔符显示在 OOBM 功能的日语区域上

表 36　英语路径分隔符出现在非英语区域中

可能原因	解决方案
底层 Intel SCS 组件中的限制。 HPCA 控制台在日语区域上显示英语路径分隔符。仅 OOBM 功能发生此问题。	没有此问题的解决方法。

无法读取或写入被管 vPro 设备

表 37　闪存限制异常错误

可能原因	解决方案
超出 vPro 存储的闪存限制。 如果对同一 vPro 设备进行多次读 / 写访问，闪存损耗保护机制会导致闪存限制异常发生。当计数器达到 200 时， vPro 设备不再允许写入操作。	使用 常用实用程序图标的下拉菜单中的**重置闪存限制**选项。有关详细信息，请参见常见实用程序的管理 （第 78 页）。

执行 vPro 操作时出现错误

表 38　vPro 操作失败

可能原因	解决方案
执行 vPro 操作时出现未授权用户或访问被拒绝等错误。	在 SCS 配置文件上启用适当的领域。

执行 DASH 操作时出现错误

表 39　DASH 操作失败

可能原因	解决方案
执行 DASH 操作时出现未授权用户或访问被拒绝等错误。	用户应有权限执行此操作。

置备

已置备 vPro 设备的状态没有按 vPro “置备”选项卡的 “设备列表”表中所示显示

表 40　vPro 状态显示问题

可能原因	解决方案
表未使用最新的信息刷新	使用 Active Directory 发现重新发现设备。设备的状态将在此操作后更新。

置备 SCS 5.0 上 AMT 固件版本低于的 4.0 的 vPro 设备时，无法设置 ACL

表 41　vPro 设备上的 ACL 配置问题

可能原因	解决方案
在为 AMT 固件为 4.0 或更低版本的 vPro 设备创建配置文件时选择了所有领域	为 AMT 固件版本较低的设备创建单独配置文件。在此配置文件中，仅选择以下领域：重定向、 PT 管理、硬件资产、远程控制、存储、事件管理器、存储、管理、代理程序存在本地、代理程序存在远程、断路器、网络时间、常规信息和固件更新。

置备 vPro 设备时控制台抛出 SCS 错误

表 42　置备 vPro 设备时发生 SCS 错误

可能原因	解决方案
从 Intel SCS 返回的内部错误。 在某些情况下，尝试通过 HPCA Console 置备 vPro 设备时，控制台抛出 SCS 错误或错误消息，但没有任何其他信息。	此错误无害，可以忽略。置备操作在 vPro 设备上已成功启动，这可在一段时间后通过验证操作结果来确认。

多次置备 vPro 设备导致控制台退出到登录屏幕

表 43　置备导致退出到登录屏幕

可能原因	解决方案
数据库访问相关问题	在某些情况下，多次尝试通过 HPCA Console 置备 vPro 设备时，控制台可能退出到登录屏幕。在这种情况下，完全关闭浏览器，然后重新登录到 HPCA Console。

发现

尽管安装了 OOBM 代理程序，还是无法发现 vPro 设备

表 44　vPro 设备发现失败

可能原因	解决方案
端口 9998 可能被防火墙阻止。	确保未在 vPro 设备上阻止端口 9998。

未发现被管 vPro 设备的硬件资产

表 45　硬件发现问题

可能原因	解决方案
在此操作期间 vPro 设备中发生内部错误	关闭设备，拔出电源线，等待 10 到 15 秒，然后重新启动设备。

表 45　硬件发现问题

vPro 设备的置备不正确	重新配置目标 vPro 设备。有关详细信息，请参见使用 MEBx 配置 vPro 设备 （第 24 页）。
容器空间限制阻止捕获其他资产数据。如果系统上存在大量设备，可以发生此问题。	断开一些设备。
由于网络流量繁重，查询硬件资产时发生网络错误	在一段时间后重新发出命令。

未发现被管 vPro 设备的软件资产

表 46　软件发现问题

可能原因	解决方案
未注册任何应用程序	安装在 vPro 设备上的软件需向 3PDS 注册。HPCA Console 不支持应用程序的注册。
由于网络流量繁重，查询软件资产时发生网络错误	在一段时间后重新发出命令。

已发现的硬件和软件资产的某些属性显示为空白

表 47　某些已发现的硬件和软件资产的值为空白

可能原因	解决方案
设备上的属性没有可用信息。	如果设备上没有存储特定属性的信息，则此行为正常。

HPCA 无法连接到 SCS，并发现 vPro 设备，在某些情况下涉及 Windows Server 2008 R2

表 48　控制台无法连接到 **SCS**，并发现 **vPro** 设备

可能原因	解决方案
原因未知。 当 Windows Server 2008-x64-R2 上安装了 HPCA 并且在运行 Windows Server 2008-x64 的同一台计算机上同时安装了 SCS 和 Active Directory 时， HPCA 无法连接到 SCS。	当 HPCA 安装在 Windows Server 2008-x64-R2 上，并且 win2k8-x64 上必须同时安装 Active Directory 和 SCS 时，请将 Active Directory 和 SCS 安装到运行 win2k8-x64 的不同物理或虚拟计算机上。

OOBM 设备数据库不具有最新设备时， OOBM 组将无法重新加载

表 49　OOBM 组未能重新加载

可能原因	解决方案
未使用最新设备更新 OOBM 数据库。 OOBM 组将无法重新加载，并会显示错误 “未找到具有给定名称的设备”。因此，将不会更新组。这会在用户通过选择**操作** > **带外管理** > **组管理** > **重新加载**执行组重新加载操作时引发问题。	再次执行 OOBM 设备发现操作以更新至最新设备。这会解决组重新加载错误。

有效 DASH 设备的发现失败

表 50　DASH 设备发现失败

可能原因	解决方案
由于网络流量的原因导致设备无法及时响应时可能发生此问题。	增加 `HTTP_READ_TIMEOUT` 和 `HTTP_CONNECT_TIMEOUT` 的配置值可能可解决此问题。在第 3 章， OOBM 配置中描述了更改配置值的过程。

使用 IP 地址而不是主机名发现和显示 DASH 设备

表 51　DASH 设备发现问题

可能原因	解决方案
设备是通过指定 IP 地址发现的，且没有针对 “反向 DNS 查找” 配置 DNS 服务器。	在尝试发现 DASH 设备时指定主机名。有关详细信息，请参见设备发现 （第 74 页）。如果没有针对 “反向 DNS 查找” 配置 DNS 服务器，将无法获得从设备 IP 地址到设备主机名的转换。所有操作需正常运行，无论显示的是 IP 地址还是主机名。

未发现已置备的 vPro 设备，或设备显示为不可用

表 52　vPro 设备发现问题

可能原因	解决方案
vPro 设备之前可能置备过，但已不再处于置备状态。	重新置备 vPro 设备。有关详细信息，请参见使用 MEBx 配置 vPro 设备 （第 24 页）。
虽然 vPro 设备仍存在于 SCS 数据库中，但可能已从域控制器中移除。	确保 vPro 设备存在于具有正确 FQDN 的域控制器中。
vPro 设备在 DNS 服务器中有多个条目。	确保 vPro 设备在 DNS 服务器中仅有一个条目。
vPro 设备在 DHCP 服务器中的 IP 地址与在 HPCA Console 的设备列表中显示的 IP 地址不同。	确保 vPro 设备在 HPCA Console 设备窗口中的 IP 地址与在 DHCP 服务器中的 IP 地址相同。

Client Automation 组中的已置备 vPro 设备未显示在 “组详细信息”窗口的 “设备”选项卡上

表 53　组设备发现问题

可能原因	解决方案
Client Automation 组中的 vPro 设备可能未使用 FQDN 列出。	通过使用 FQDN 并将此设备添加到组，从而将设备导入 Client Automation 组。然后将 Client Automation 组重新加载到 HPCA Console 中。

远程操作

在 DASH 设备上执行远程操作时， PuTTY 控制台未能打开

表 54　PuTTY 控制台不打开

可能原因	解决方案
另一个 PuTTY 控制台可能正在系统上运行。在启用显示到控制台选项的情况下执行 DASH 远程操作时，如果另一个 PuTTY 控制台正在系统上运行， PuTTY 控制台将无法打开。	在执行 DASH 远程操作之前，确保没有其他 PuTTY 控制台正在运行。

执行远程操作时， Telnet 控制台未打开

表 55　Telnet 控制台不打开

可能原因	解决方案
特定 Internet 设置不正确，阻止了 Telnet 控制台的显示	在 Internet Explorer 中，转到**工具 > Internet 选项 > 高级**。确保选中**禁用脚本调试 (Internet Explorer)** 和**禁用脚本调试 （其他）**选项。
ActiveX 控件的默认安全设置阻止了 Telnet 控制台的显示	在 Internet Explorer 中，转到**工具 > Internet 选项 > 安全**。单击**自定义级别**。对于**下载未签名的 ActiveX 控件**和**对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本**，选择 “启用”。

Telnet 会话无法在 Windows Server 2003 64 位平台上的客户端控制台上打开

表 56　Telnet 会话不能在 Windows Server 2003 64 位系统上打开

可能原因	解决方案
OOBM 无法在此平台上打开 Telnet 连接。	使用 HyperTerminal 查看 vPro 设备文本控制台。配置 PuTTY 客户端查看 DASH 设备文本控制台。

PuTTY 客户端可能无法在 Windows 64 位平台上显示 DASH 客户端控制台

表 57　PuTTY 客户端无法在 Windows 64 位系统上显示 DASH 客户端控制台

可能原因	解决方案
PuTTY 无法与 Windows 64 位系统上的客户端 DASH 设备建立连接。	没有此问题的解决方法。

更改设备的置备状态之后， vPro 设备上的 OOBM 远程操作失败

表 58　在更改置备之后，远程操作在 vPro 设备上失败

可能原因	解决方案
OOBM 数据库与 SCS 数据库中的信息不一致。 更改 vPro 设备的置备状态 （包括更改 TLS 模式、使用不同的 SCS 配置文件重新置备设备等）时，单个或多个 vPro 设备上的远程操作失败。	选择置备状态已更改的设备并从**操作 > 带外管理 > 设备管理**单击**重新加载设备信息**按钮。或者，在不选择设备的情况下单击**重新加载设备信息**按钮。后者所需时间更长，但将会刷新所有设备信息，因此 OOBM 数据库中加载的是最新信息，并且此信息与 SCS 数据库中的信息一致。

在 vPro 设备上执行 OOBM 远程操作时，未产生任何效果

表 59　执行远程操作时，没有响应

可能原因	解决方案
• OOBM 数据库与 SCS 数据库中的信息不一致 • 网络上的设备不可用	关闭 “设备详细信息” 窗口，然后重新打开一个窗口。这会允许您看到错误消息。如果问题由 OOBM 和 SCS 数据库之间的不一致引起，则在**操作** > **带外管理** > **设备管理** > **全部刷新**下单击**重新加载设备信息**按钮。

无论引导顺序如何， OOB DASH 设备都从硬盘引导

表 60　DASH 设备始终从硬盘引导

可能原因	解决方案
基于 Broadcom NetExtreme Gigabit Ethernet Plus NIC 硬件的问题。 如果用户在引导顺序中已包含 USB，并且如果 USB 引导源不可引导，则系统将从硬盘引导而不管引导顺序中的其他引导源。这将在用户通过选择**操作** > **带外管理** > **设备管理** > *<DASH 设备 >* > **远程操作**在 DASH 设备上执行引导操作时引发问题。	尚无解决方法。

OOB DASH 设备尝试所有引导源，包括未在引导顺序中指定的引导源

表 61　DASH 设备尝试所有引导源，而不管引导源是如何指定的

可能原因	解决方案
基于 Broadcom NetExtreme Gigabit Ethernet Plus NIC 的硬件的问题 如果用户选择持久引导选项，则设备将尝试所有引导源，包括未在引导顺序中指定的引导源。这将在用户通过选择**操作** > **带外管理** > **设备管理** > *<DASH 设备 >* > **远程操作**在 DASH 设备上执行引导操作时引发问题。	尚无解决方法。

错误的网络控制器设置为 OOB DASH 设备的第一引导源

表 62　错误的网络控制器设置为 DASH 设备的第一引导源

可能原因	解决方案
基于 Broadcom NetExtreme Gigabit Ethernet Plus NIC 硬件的问题。 对于已启用 Dash 的设备，如果更改引导顺序以使得网络为第一引导设备，则引导顺序会将嵌入的网络控制器（而不是 Broadcom DASH NIC）设置为第一引导源。因此，从 Broadcom NIC 的 PXE 引导将失败。	转到 F10 高级设置菜单中。通过禁用 “设备选项”列表中的 “NIC PXE 选项 ROM 下载”选项，可以阻止嵌入的 NIC PXE 选项 ROM 进行加载。禁用此选项之后，重新尝试从 Broadcom PXE 引导。

从 “远程操作向导任务”页无法转到下一页

表 63　远程操作向导冻结问题

可能原因	解决方案
JRE 的版本错误	安装 JRE 版本 1.5 或更高版本，并在 Internet Explorer 中选择用于安装 JRE 插件的选项。要选择此选项，请在 Internet Explorer 中转到**工具 > Internet 选项 > 高级**，然后选中**将 JRE 1.5.*XX* 用于 <applet>（需要重新启动）**选项。安装并启用 JRE 之后，请重新启动 Internet Explorer。

无法为 vPro 设备上的 SOL/IDE-R 操作打开 Telnet 会话

表 64　无法为 SOL/IDE-R 操作打开 Telnet 会话

可能原因	解决方案
Telnet 客户端可能未安装。默认情况下，不在 Windows Server 2008 上安装 Telnet 客户端。 当 HPCA 安装在 Windows Server 2008 x64 (AMD64T) 上时，不会为 SOL/IDER 操作打开 Telnet 会话。但是，引导操作已成功执行，并且计算机从正确的介质引导。由于此问题，不会完全支持修复用例。例如， BIOS 更新无法执行。	通过使用 Windows Server 2008 中的服务器管理器选项来安装 Telnet 客户端。

DASH 设备的 “远程操作向导” 一直显示进度条，而不显示操作完成

表 65 “远程操作向导” 一直显示进度条

可能原因	解决方案
设备硬件没有向导致一直等待的 “远程操作向导” 的远程操作发送确认。但是，远程操作已成功。	要执行其他 OOBM 远程操作的唯一方法是注销，关闭当前 IE 会话，然后在新的 IE 会话中重新登录。

DASH 设备的引导配置设置仍保持启用一段时间

表 66 DASH 设备的引导配置设置保持启用

可能原因	解决方案
这反映出操作仍在进行中并将最终完成。	此行为是期望行为。

诸如休眠 （软）和暂挂等远程操作在目标 DASH 设备上不可用

表 67 休眠和暂挂操作在 DASH 设备上不可用

可能原因	解决方案
Broadcom 管理代理程序可能未在目标 DASH 设备上运行，或者 DASH 设备可能未处于 Windows 操作系统运行状态。如果存在以上任意情况，则休眠和暂挂操作在 DASH 设备将不可用，即使操作在 HPCA Console 中显示为成功。	确保已安装最新 Broadcom 管理代理程序，且管理代理程序服务在目标 DASH 设备上的 Windows 中运行。

vPro 设备 IDE-R 操作信息在 HyperTerminal 控制台中未正确对齐

表 68 IDE-R 信息在 HyperTerminal 中未对齐

可能原因	解决方案
硬件供应商的定时问题或固件问题。	没有此问题的解决方法。

多个用户在同一 OOBM 设备上执行操作导致不稳定行为

表 69 多个用户在同一设备上执行操作

可能原因	解决方案
结构限制。	在任何给定的时间，都只允许一个用户在设备上执行远程操作。

vPro 设备在 IDE-R 重新启动后未关闭电源

表 70　IDE-R 重新启动后 vPro 设备的关闭电源问题

可能原因	解决方案
Web 服务忙于执行当前操作	vPro 在 IDE-R 重新启动后可能无法成功执行电源关闭命令。请等待十秒钟然后再发出电源关闭命令，应当可以解决此问题。

vPro 设备软 IDE-R 重新启动生成输出到 SOL 显示的难解信息

表 71　vPro 设备生成输出到 SOL 的难解信息

可能原因	解决方案
导致此问题的原因可能是因为可引导软盘是从 MS Windows 版的 MS-DOS （例如，在 Windows 中使用 Format 创建 MS-DOS 启动磁盘）创建的。	使用其他方式创建可引导软盘驱动器。

在执行电源关闭命令后， vPro 设备变为灰显

表 72　关闭电源后 vPro 设备变为灰显

可能原因	解决方案
ME 电源设置选项的设置可能不正确。在 SCS 配置文件中，电源策略的设置可能不正确。而且，vPro 设备在 DNS 服务器中可能有多个条目。	确保在所有可能的电源状态中， ME 电源设置选项设置为始终在 ME 上，或在 ME 上唤醒。并检查 SCS 配置文件，以确保电源策略设置为始终开启。最后，检查 vPro 设备在 DNS 服务器中是否有多个条目。如果有多个条目，删除错误条目，重新启动 DNS 服务器，清除 HPCA Console 服务器中的 DNS，然后重新启动 HPCA Console 服务器。或者，可以提高 HPCA 服务器上的 Web 服务超时值。

OOB 设备转变为 S1/S2 或休眠灯电源状态显示不稳定行为

表 73　S1/S2 或休眠灯电源状态显示不稳定行为

可能原因	解决方案
部分硬件供应商不支持 S1/S2 或休眠灯电源状态。	有关详细信息，请参见硬件供应商文档。

OOB 设备在电源关闭后滞于暂挂状态

表 74　设备在电源关闭后滞于暂挂状态

可能原因	解决方案
在某些硬件上，如果系统在暂挂状态时用户调用电源关闭命令，则 HPCA Console 报告成功，但计算机滞于暂挂状态中。这是由于在这些情况中，硬件不支持在暂挂状态中执行电源关闭操作。	如果遇到此类行为，请参见硬件供应商文档以获取更多详细信息。

DASH 设备上的有序电源操作显示为支持的选项，但不可用

表 75　有序远程操作在 DASH 设备上不可用

可能原因	解决方案
未安装 Broadcom 管理代理程序	在 DASH 设备上安装最新 Broadcom 管理代理程序。

执行 KVM 操作时出现错误

表 76　KVM 操作失败

可能原因	解决方案
执行 KVM 操作时出现未授权用户或访问被拒绝等错误。	在 SCS 配置文件上启用 PT Administration 领域并重新置备 vPro 设备。

电源状态

无法查看或更改被管 vPro 设备的电源状态

表 77　电源状态问题

可能原因	解决方案
由于网络流量繁重，查询系统时发生网络错误	在一段时间后重新发出命令。
由于活动 IDE-R/SOL 会话，电源关闭失败	存在活动 IDE-R/SOL 会话时不支持电源关闭命令。控制台抛出“参数有效但平台不支持”异常。检查是否有活动会话。如果有，关闭该会话，并在一段时间后尝试关闭电源。

在电源关闭操作后设备的电源状态变为灰显

表 78　电源显示问题

可能原因	解决方案
超过超时期间	重新配置超时期间。有关详细信息，请参见配置 IDE-R 和 SOL 超时值 （第 34 页）。

重新启动

要对重新启动问题进行疑难解答，必须检查 IDE-R 和 SOL 的全局配置设置和远程控制选项。

对于一次性引导设置，重新启动 OOB DASH 设备之前必须执行引导顺序操作

表 79　必须在重新引导 DASH 设备之前执行引导顺序操作

可能原因	解决方案
基于 Broadcom NetExtreme Gigabit Ethernet Plus NIC 硬件的问题。 对于基于 Broadcom NetExtreme Gigabit Ethernet Plus NIC 硬件上的重新启动操作，如果用户选择一次性引导的引导配置设置，则在重新启动之前，用户需要执行引导顺序操作。否则，远程操作将显示不稳定的行为。另请注意，尽管用户已执行明确的引导顺序操作，但在重新启动之后，引导顺序将重置为默认引导顺序。这将在用户通过选择**操作** > **带外管理** > **设备管理** > <*DASH 设备*> > **引导配置**在 DASH 设备上执行引导操作时引发问题。	尚无解决方法。

在 OOBM DASH 设备上，一次性引导配置未重置

表 80　一次性引导配置未在 DASH 设备上重置

可能原因	解决方案
系统 BIOS 问题。 即使设备重新启动之后，DASH 设备上的一次性引导配置也未重置。为任意远程操作选中或启用一次性引导配置时，一旦远程操作成功完成之后，此配置仍处于选中或启用状态。一旦发生此问题，所有后续的远程操作将一直使用该一次性引导配置。这将在用户通过选择**操作** > **带外管理** > **设备管理** > *<DASH 设备* > > **引导配置**在 DASH 设备上设置一次性引导配置时引发问题。	通过选择**操作** > **带外管理** > **设备管理** > *<DASH 设备* > > **远程操作**执行任何重新启动操作之前，更改一次一个引导配置的引导顺序。

无法将 DASH 设备的引导配置设置更改为默认和持久引导

表 81　无法更改 DASH 设备上的引导配置

可能原因	解决方案
这些设置对于列出的第一个引导配置设置的持久引导配置设置为硬编码。 不可能将引导配置设置更改为默认和持久引导。用户无法将此设置更改为一次性引导。但是，用户可以将列出的第二个引导配置设置的设置更改为一次性引导。这将在用户通过选择**操作** > **带外管理** > **设备管理** > *<DASH 设备* > > **引导配置**在 DASH 设备上执行引导配置设置时引发问题。	没有此问题的解决方法。

使用 SOL 在 HPCA Console 上看不到重新启动过程

表 82　使用 SOL 查看重新启动的问题

可能原因	解决方案
端口 9999 已由其他设备使用	释放端口 9999 以用于 SOL 传输。
SOL 重定向在置备期间未启用	使用 Intel SCS 启用 SOL 重定向。有关详细信息，请参见使用 MEBx 配置 vPro 设备（第 24 页）。
使用 Windows 资源管理器创建的可引导软盘	使用 Windows 中的 Format 创建 MS-DOS 启动磁盘可生成可引导驱动器，但是输出到 SOL 的信息无法理解。使用其他方式创建可引导软盘驱动器。

无法远程重新启动被管 vPro 设备

表 83　重新启动问题

可能原因	解决方案
重新启动参数不正确	查看日志以检查重新启动参数。如果参数不正确，尝试使用正确参数重新启动。
某些选项的固件中的已知限制	检查 HPCA Core 分发介质上 `Media\oobm\win32\AMT Config Server` 目录中的 Intel vPro SCS Server 的发行说明。

表 84　IDE-R 重新启动问题

可能原因	解决方案
管理控制台中不存在物理可引导设备 （驱动器 / 映像）。	引导到管理控制台中的现有驱动器。如果没有物理设备，则使用 ISO 映像。
介质中的映像不可引导。	检查映像是否可引导。如果不能，改用可引导映像。
如果尝试重新启动到 CD/DVD，则 HPCA Console 服务器上的 CD 驱动器不匹配默认的 `D:` 驱动器设置。	重新配置默认驱动器设置以匹配 HPCA Console 服务器上的 CD/DVD 驱动器。有关详细信息，请参见配置 IDE-R 驱动器 （第 33 页）。

无法远程重新引导被管 vPro 设备到 BIOS 设置

表 85　重新引导到 BIOS 设置的问题

可能原因	解决方案
BIOS 不支持引导到 BIOS 设置	将目标设备上的 BIOS 升级到支持此功能的 BIOS 版本。

无法重置被管 vPro 设备的引导顺序

表 86　重置引导顺序的问题

可能原因	解决方案
难以确定	执行本地 HDD 引导命令，并重新启动目标设备。

系统防御和代理程序存在

无法将统防御策略部署到被管 vPro 设备

表 87　添加系统防御网络过滤器错误

可能原因	解决方案
已超出 vPro 设备的 31 个入站和 30 个出站过滤器限制	删除 vPro 设备上的一些现有过滤器。有关详细信息，请参见管理系统防御过滤器（第 54 页）。

在使用无线网络驱动程序时，系统防御策略在 vPro 设备上有时无法正常工作

表 88　具有无线 NIC 的设备上的系统防御策略

可能原因	解决方案
vPro 设备上的无线网络驱动程序版本与安装的 Intel AMT 版本不一致。	为保证系统防御策略的正常运行，vPro 设备上的无线网络驱动程序版本必须与安装的 Intel Active Management 技术的版本一致。关于版本兼容性的更多详细信息可从硬件供应商处获得。

无法在被管 vPro 设备上部署监视程序

表 89　监视程序部署错误

可能原因	解决方案
vPro 设备上只能部署一个 OOBM 代理监视程序。可以部署多个第三方代理监视程序， vPro 设备上安装的每个第三方代理程序一个。单个设备上可以部署的监视程序总数是 16。	从 vPro 设备移除或取消部署监视程序。有关详细信息，请参见管理监视程序 （第 64 页）。
为监视程序定义了无效、矛盾的操作。	复查为监视程序指定的操作，并修改矛盾之处。有关详细信息，请参见管理监视程序（第 64 页）。

OOBM 代理程序安装失败，返回错误代码 1920

表 90　OOBM 代理程序安装错误

可能原因	解决方案
之前安装或卸载 OOBM 代理程序的问题。	从 vPro 设备移除 HPCA-OOBM 代理程序服务。要执行此操作，右键单击 “我的电脑” 图标，浏览至**管理** > **服务和应用程序** > **服务**。检查 HPCA-OOBM 代理程序服务。如果此服务存在，执行以下操作： • 打开命令提示符窗口 • 输入 **`sc delete HPCA-OOBM`** • 重新启动系统
在安装 OOBM 代理程序时未提供用户名和密码。	提供 “虚设” 用户名和密码，即使不希望使用延迟的配置置备设备。如果不提供用户名和密码，安装将失败，返回错误代码 1920。

OOBM 代理程序关闭

表 91　OOBM 代理程序关闭行为

可能原因	解决方案
未定义要监视的应用程序。	创建并部署要 OOBM 代理程序监视的应用程序软件列表。有关详细信息，请参见管理监视程序（第 64 页）。

在 vPro 设备上部署 OOBM 代理程序软件列表时抛出 SOAP 错误

表 92　部署代理程序软件列表导致 SOAP 错误

可能原因	解决方案
vPro Web 服务返回错误。 OOBM 代理软件列表的部署可能引发以下几个错误中的一个错误：“网络错误 – SOAP 错误代码：22”、“完整性检查错误”、“尚未初始化” 和 “无效参数”。	在一段时间后重试同一操作。如果错误仍旧存在，请注销后重新登录到 HPCA Console。

OOBM 代理程序在 vPro 设备的软件列表中不显示

表 93　代理程序不在 vPro 设备的软件列表中

可能原因	解决方案
如果 OOBM 代理程序由一个用户帐户安装，当使用其他帐户登录的用户查看时，会发生结构限制。	没有此问题的解决方法。

向 vPro 设备上的一个 NIC 部署代理程序存在策略时，多个 NIC 返回错误

表 94　在具有多个 NIC 的 vPro 设备上部署代理程序存在策略

可能原因	解决方案
内部错误。	将代理程序存在策略部署到这两个 NIC 上，然后从不需要的 NIC 取消部署代理程序存在策略。

反电子欺诈过滤器导致 vPro 设备上的所有传出流量断开

表 95　反电子欺诈过滤器导致所有传出流量断开

可能原因	解决方案
如果 vPro 设备在启用了环境监测的 SCS 中制备了配置文件，并且该设备连接到域，此域尚未在环境检测域中指定，则若 vPro 设备上的系统防御策略启用了反电子欺诈过滤器，所有传出流量将断开。	将设备连接到环境检测域中指定的域。

OOBM 代理程序无法向 vPro 设备上的监视程序注册

表 96　OOBM 代理程序注册问题

可能原因	解决方案
如果 OOBM 代理程序无法向监视程序注册，问题可能出在 Digest 用户名（Intel AMT 用户名）上。在 Intel AMT 固件中， Digest 用户名区分大小写。安装 OOBM 代理程序时，必须使用准确的大小写指定 Digest 用户名。否则，OOBM 代理程序将无法成功向监视程序注册。	确保使用准确的大小写正确指定 Digest 用户名。

vPro 设备的 OOBM 代理程序停止时，重复显示消息

表 97　当停止 OOBM 代理程序时出现重复消息

可能原因	解决方案
HPCA-OOBM 代理程序中的内部错误	如果出现此情况，重新启动客户端 vPro 设备上的 HPCA-OOBM 代理程序服务 (HPCA-OOBM)。

在更改 Digest 凭据后，无法访问 vPro 设备

表 98　在更改凭据后，无法访问 vPro 设备

可能原因	解决方案
代理程序仅在安装时获取密码，不会在密码更改时动态获取密码。 如果已经通过 SCS Console 更改了此设备的 Digest 用户名/密码，则将无法访问 vPro 设备。	在更改 Digest 凭据后，若要能够访问和管理此设备，必须在 vPro 设备上停止 OOBM 代理程序 (HPCA-OOBM) 服务。如果您使用代理程序存在功能，则必须使用新密码在 vPro 设备上重新安装 OOBM 代理程序。

在从 TLS 配置文件更改为非 TLS 配置文件后， vPro 设备上的 OOBM 代理程序无法正常工作

表 99　OOBM 代理程序和 TLS 配置文件

可能原因	解决方案
如果 OOBM 代理程序是使用 TLS 配置文件安装的，并且在某个时刻使用非 TLS 配置文件重新置备了 vPro 设备，则 OOBM 代理程序将无法正常工作。同样，如果 OOBM 代理程序是使用非 TLS 配置文件安装的，并且在某个时刻使用 TLS 配置文件重新置备了 vPro 设备，则 OOBM 代理程序将无法正常工作。	如果发生此情况，则必须使用适当的配置文件重新安装 OOBM 代理程序。

OOBM 代理程序管理弹出消息一闪而过

表 100　OOBM 代理程序管理消息显示

可能原因	解决方案
如果激活了代理程序存在策略，这是管理弹出消息的默认行为。	在 vPro 设备上打开 Windows 事件查看器，查看所有与代理程序相关的日志消息。

无法在被管 vPro 设备上部署 OOBM 代理程序软件列表和系统消息

表 101 部署 OOBM 代理程序软件列表和系统消息错误

可能原因	解决方案
• 对 3PDS 的多个操作同时发生 • 在一个会话中多个访问 3PDS • 通过网络的数据传输问题	在一段时间后重试部署。

无法部署 OOBM 代理程序软件列表或在 TLS 模式中查看软件信息

表 102 TLS 模型中的 OOBM 代理程序问题

可能原因	解决方案
Tomcat 服务可能未在域管理员帐户上运行。	确保 HPCA Tomcat 服务器服务在域管理员帐户上运行。如果不是，重新配置并重新启动 Tomcat。
证书授权机构 (CA) 上指定的常用名称可能不正确。	确保正确指定了 CA 上的常用名称。此设置可在安装目录中的 `local_settings.ini` 文件中找到。

在成功安装 OOBM 代理程序后， HPCA Console 上的监视程序状态未更改。

表 103 监视程序注册错误

可能原因	解决方案
监视程序注册失败。	在 vPro 设备上打开 Windows 事件查看器，检查监视程序注册日志消息。如果不成功，在 vPro 设备上安装主机嵌入式控制器接口 (HECI) 驱动程序和本地可管理性服务 (LMS) 服务，然后重新检查监视程序状态。

执行定义的操作后，已部署的代理程序存在策略未激活

表 104 代理程序存在策略未激活

可能原因	解决方案
定义的操作可能未按预期顺序执行。 OOBM 代理程序可能在转换为指定状态之前已过期。	最保险的做法是在指定监视程序操作时，将“不关心状态”指定为转换后的状态。

代理程序存在策略在部署后立即激活

表 105 代理程序存在策略立即激活

可能原因	解决方案
激活代理程序存在策略的转换状态可能已出现，促使监视程序立即激活代理程序存在策略。	删除现有监视程序并重新部署。

名称中包含特殊字符时无法部署系统防御策略

表 106 系统防御策略名称错误

可能原因	解决方案
创建过滤器和策略时可以在名称中使用非 ASCII 字符，但将无法部署它们。同样，无法部署名称中带有特殊字符（如“:”、“,”、“>”、“<”、“&”及“”的过滤器和策略。此限制在 Intel AMT 规范中已指出。	创建过滤器和策略时使用符合规范的名称。

无线

无法通过 HPCA Console 连接到无线设备

表 107 无线设备连接问题

可能原因	解决方案
由于建立与无线设备通信花费的时间过长，发生 Web 服务超时。当 HPCA Console 无法连接时，设备在控制台中变为灰显。	重新配置超时期间。有关详细信息，请参见配置 IDE-R 和 SOL 超时值（第 34 页）。

无法使用无线 NIC 连接到 vPro 设备

表 108 无法使用无线 NIC 连接

可能原因	解决方案
仅配置无线 NIC 时和设备未插电源及未开机时， 2.5 版 vPro 设备的预期行为。	将 vPro 设备连接到电源并通电。

在无线网络上为 vPro 设备建立 SOL/IDE-R 会话失败

表 109 通过无线网络的 SOL/IDE-R 会话失败

可能原因	解决方案
由于使用无线 NIC 的 vPro 设备需要大量时间与 OOBM 服务器通信，因而发生超时。	按照配置 IDE-R 和 SOL 超时值（第 34 页）所述，配置 `IDER*` 和 `SOL*` 参数。

无线 NIC 的策略设置失败

表 110 无线策略部署问题

可能原因	解决方案
vPro 设备没有无线 NIC，但是策略显示为已经成功部署。	取消部署策略，或在 vPro 设备上安装无线 NIC，然后重新部署策略。

迁移问题

迁移到 SCS 5.3 后， SCS 控制台未正确显示配置文件

表 111 显示配置文件时发生 SCS 迁移问题

可能原因	解决方案
SCS 数据已从 SCS 的以前版本迁移。在这种情况下，新 SCS 控制台不会在左侧树视图中显示迁移后的配置文件。	可以在 SCS 控制台左侧的配置文件部分中查看配置文件信息。

OOBM 代理程序软件列表和系统消息在迁移到当前版本的带外管理软件后无法显示

表 112 OOBM 代理程序消息和列表的迁移问题

可能原因	解决方案
这是正常行为。如果 OOBM 代理程序的软件列表和系统消息是在早期版本的带外管理软件中创建和部署的，在迁移到更高版本后，它们将不可用。	在当前版本中创建并重新部署 OOBM 代理程序和系统消息。有关详细信息，请参见管理监视程序 （第 64 页）。

迁移到更高发行版时，增量发现执行完全发现

表 113 迁移到更高发行版时执行设备发现

可能原因	解决方案
此行为是期望行为。	从更早版本迁移时，迁移的设备将在 HPCA Console 中列出。第一次执行 vPro 发现（完整/更新发现）时，将执行完整 vPro 发现（并非增量更新），因为它是在控制台的当前版本中执行的第一个发现。

备份 OOBM 数据

最好能坚持定期备份 OOBM 数据。有三种类型的文件需要备份：

- 配置文件
- 数据文件
- 数据库

HPCA 的默认安装目录是 `C:\Program Files\Hewlett Packard\HPCA`。HPCA 的默认数据目录是 `C:\Program Files\Hewlett Packard\HPCA\data`。

➤ 如果在卸载或升级 HPCA 时要保留 OOBM 配置和数据文件以供以后使用，则必须使用迁移脚本进行备份和文件还原。有关迁移和还原的详细信息，请参见在分发介质的 `Documentation\HPCA Standard\Migration Guides` 下提供的《HP Client Automation Starter 和 Standard Edition 迁移指南》(HP Client Automation Starter and Standard Edition Migration Guide)。

配置文件

备份配置文件

OOBM 配置文件，即 `configuration.properties` 和 `config.properties`，位于 *<HPCA_INSTALL_DIR>*`\oobm\conf` 中。将这些两个文件复制到 HPCA 安装目录结构以外的位置。如果在重新安装 HPCA 产品时要保留现有配置，则可以将它们复制回原始位置。

数据文件

备份数据文件

过滤器、策略、启发和监视程序的所有 vPro 系统防御配置信息以 XML 文件形式放置在 `<HPCA_DATA_DIR>\oobm\datafiles` 中。将 `sd.xml` 和 `AgentPresence.xml` 文件复制到 HPCA 安装目录结构以外的位置。如果在重新安装 HPCA 产品时要保留现有 vPro 系统防御配置信息，则可以将它们复制回原始位置。

数据库

备份数据库

OOBM 数据库存储发现的设备、 DASH 凭据和 HPCA 组的有关信息。此数据库位于 `<HPCA_DATA_DIR>\oobm\OOBMDB` 中。将整个 `OOBMDB` 目录复制到 HPCA 安装目录结构以外的位置。如果在重新安装 HPCA 产品时要保留此信息，则可以将此目录复制回原始位置。

端口信息摘要

带外管理使用多个 TCP 端口进行通信。如果安装了公司或个人防火墙软件，那么必须在 HPCA Console 服务器上排除以下端口以允许入站和出站流量。

对于带外管理服务与 vPro 设备的通信：

- 经由 TCP 的 Web 服务流量使用端口 16692。
- 经由 TLS （具有客户端验证）的 Web 服务流量使用端口 16693。
- 使用端口 9999 作为 SOL 显示小程序和服务器的 Web 应用程序之间通信的默认起始端口。此端口是可配置的。
- 经由 TCP 的 SOL/IDE-R 使用端口 16694。
- 经由 TLS （具有客户端验证）的 SOL/IDE-R 使用端口 16695。
- 警告管理使用端口 162。

对于浏览器与服务器的通信：

- 小程序与服务器套接字 SOL 通信使用端口 9999。此端口在客户端浏览器系统上必须同样可用。
- vPro 设备上用于 KVM 重定向的 VNC Viewer 使用端口 5900。

对于带外管理服务与 OOBM 代理程序的通信：

- 在远程配置 vPro 设备期间，带外管理和 OOBM 代理程序之间的通信使用端口 9998。

对于带外管理服务和 DASH 设备：

- 带外管理和 DASH 设备之间的通信使用端口 623。

清单问题

如果在 HPCA Console 中仍有与带外管理功能相关的问题，请致电 HP 支持。在打电话之前，请确保知道以下问题的答案。此信息将帮助支持团队更快地解决您遇到的问题。

1 HPCA Console 服务器上安装的操作系统和 Service Pack 是什么？

2 SCS Server 上的 IIS 版本是什么？

3 SCS 和 HPCA Console 是否安装在同一台计算机上？

4 SCS 和 SQL Server 是否安装在同一台计算机上？

5 网络中是否安装了 Active Directory？

6 您的网络是否启用了 DNS 和 DHCP？

7 SCS 和 HPCA Console 上的带外管理服务之间的验证是否使用了 NTLM v2 协议 （可检查以确认本地策略）？

8 安装 SCS 时使用的用户标识是什么 （无论是本地用户还是域用户）？

9 该本地或域用户是否拥有本地管理员权限？

10 与 SQL 通信时使用的验证模式是什么 （建议使用 Windows 验证）？

11 能否登录到 HPCA Console？

12 HPCA Console 中 “设备” 选项卡上是否列出了任何设备？

13 设备是否是已显示但被禁用，即变为灰显并不可访问？

14 是否有使用 SCS 置备的设备？

15 SCS 表中是否列出了已置备的设备？

16 在登录 SCS 时，是否使用了 **http://IP/AMTSCS** 或 **https://IP/AMTSCS** 作为 URL？

A OOBM 功能

通过 HPCA Console 中的带外管理 (OOBM) 选项，可以对网络中置备的设备执行发现、修复和保护操作 （取决于设备类型）。

下面各节介绍可用来发现、修复和保护网络上的 OOB 设备的 OOBM 功能。

➤ 保护功能仅适用于 vPro 设备。

发现

您可以发现网络上所有已置备 OOB 设备中的硬件资产和软件资产。

硬件资产

Intel vPro 设备将硬件资产信息存储在闪存中。DASH 设备将此信息存储在网络控制器的 NVRAM 中。可以随时对这两者进行读取 （即使在电源已关闭的情况下）。唯一的条件是设备必须以物理方式接入网络，并接通电源。 OOB 设备不依赖于软件代理程序，以防止意外丢失数据。您可以通过 HPCA Console 访问此信息，并使用它执行以下操作：

- 确定设备上任何可能需要更换的硬件组件的确切规格。
- 识别兼容性问题。
- 在设置新操作系统之前检查设备的配置。
- 检索特别库存信息，即使计算机已关闭。

软件资产

Intel vPro 允许您查看 vPro 设备上已向第三方数据存储 (3PDS) 注册的应用程序的列表。对于已向 3PDS 注册的 HP 应用程序，还可以查看这些应用程序已写入 vPro 设备的暂存区域的数据。DASH 设备将软件资产信息存储在网络控制器的 NVRAM 中。您可以通过 HPCA Console 访问此信息，并使用它执行以下操作：

- 确定设备上是否安装有采用 vPro 或 DASH 技术的应用程序。数据存储的确切使用取决于应用程序。
- 在带外信息中检索 vPro 和 DASH 感知的 HP 应用程序。
- 确认 vPro 和 DASH 感知的应用程序是否注册正确。这有助于排除某些应用程序故障。
- 确认 vPro 和 DASH 感知的 HP 应用程序是否正确工作。

- 查看希望 vPro 设备上运行的 OOBM 代理程序去监视的应用程序软件列表。
- 如果激活代理程序存在策略，则可以查看 OOBM 代理程序将向 vPro 设备控制台显示的系统消息。

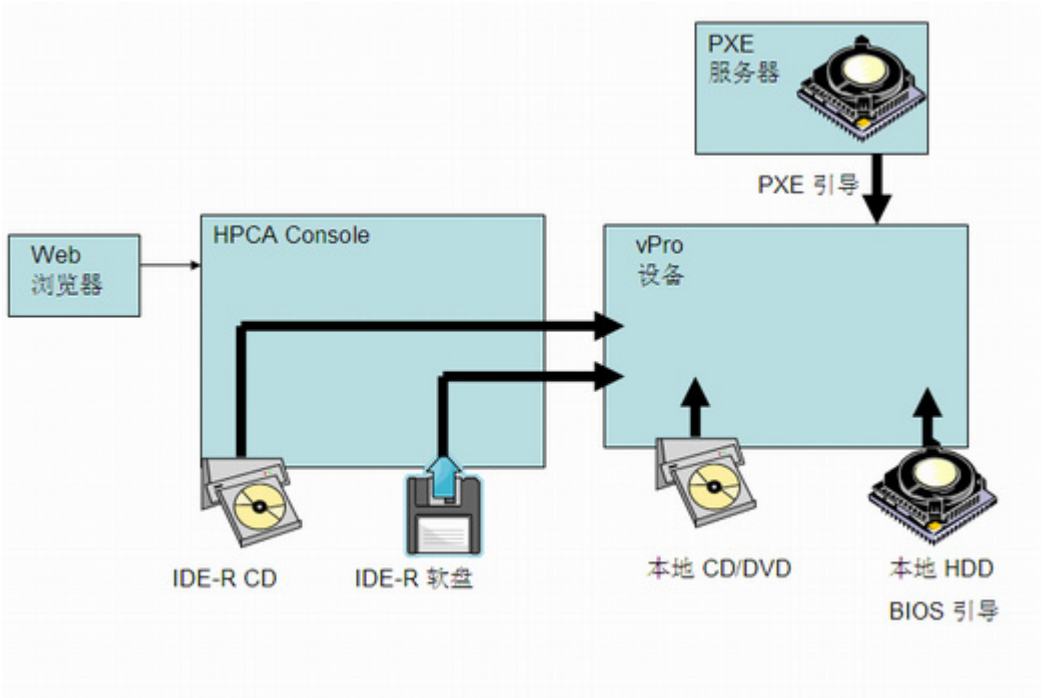
修复

修复操作包括远程操作和事件管理。

事件管理只与 vPro 设备有关。

下图说明了可以通过 HPCA Console OOBM 选项执行的各种远程管理操作（IDE-R 只适合于 vPro 设备）。

图 3　远程管理操作概述



远程操作

Intel vPro 和 DASH 设备提供带外访问功能，以便在软件、操作系统和硬件发生故障之后对设备进行远程诊断和修复。通过 HPCA Console，可以远程查看设备电源状态，从硬盘重新启动，从本地 CD/DVD 的映像中重新启动，从远程 CD 或软盘驱动器中重新启动，从 PXE 服务器重新启动，以及重新启动到 BIOS 设置。执行任何远程操作或者系统处于空闲状态时，系统的电源状态都会发生变化。

您可以使用这些功能执行远程电源管理操作，其中包括：

- 打开和关闭设备电源

- 使用控制台文本重定向和 IDE-R 重新启动 OOB 设备

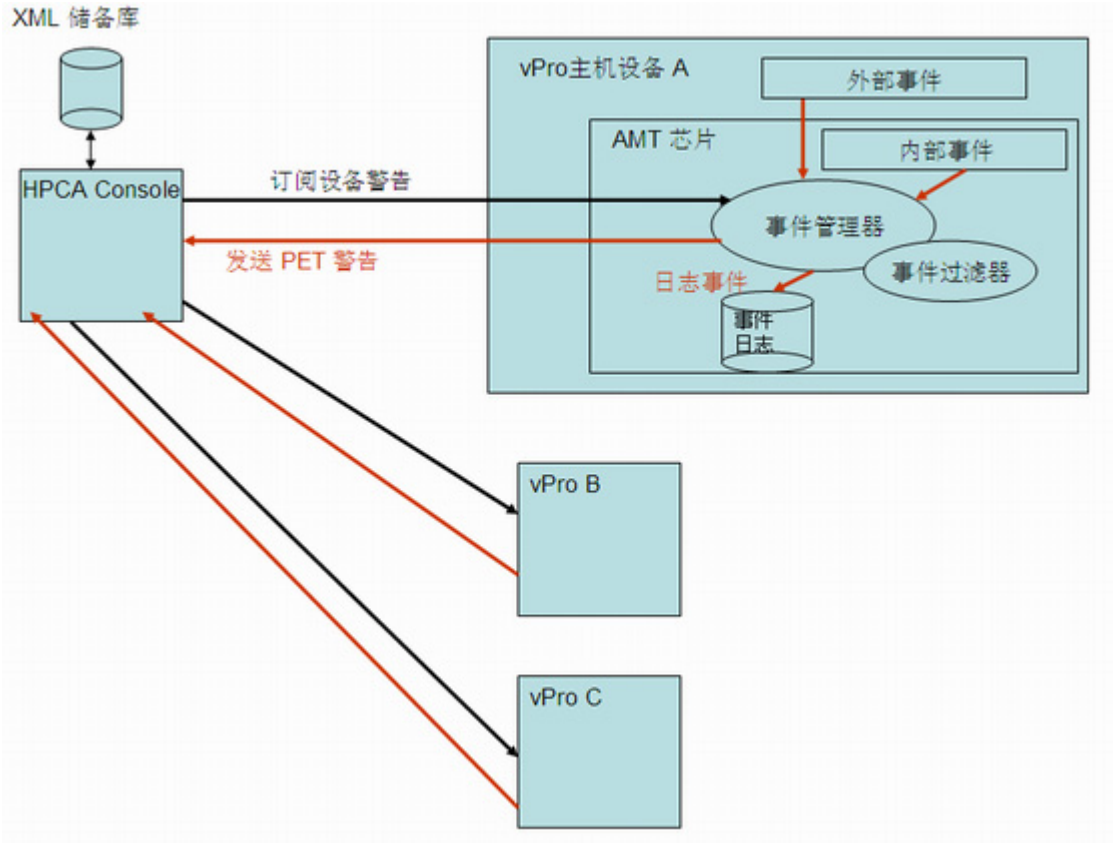
电子集成驱动器重定向 (IDE-R) 仅适用于 vPro 设备。

电源管理操作允许将有问题的 OOB 设备还原到正常状态。

事件管理

下图说明了 vPro 系统的事件管理中涉及的动态关系。

图 4　事件管理概述



Intel vPro 支持警告和事件日志记录，以帮助快速诊断问题，缩短终端用户的停机时间。事件是从系统管理 (SM) 总线和硬件传感器等外部源中生成的。还有 vPro 自身生成的内部事件。内部事件存在多个源。它们包括由系统防御过滤器、代理程序存在失败、固件更新和多个其他方案触发的事件。因此，事件可以是实际发生的 （比如风扇故障）也可以是过滤器检测到的 （由于流量模式的改变，比如病毒攻击）。如果系统上发生某个事件，驻留在 vPro 芯片上的事件管理器会引发事件，并访问事件过滤器以确定采取何种操作。事件过滤器定义一组应用于每个传入平台事件的条件。如果传入事件与条件匹配，事件过滤器会指定要采取的操作。这些操作可以包括将警告发送到 HPCA Console 和 / 或将事件记录在 vPro 日志。

您必须订阅 vPro 设备，这样该设备生成的事件警告才会发送到 HPCA Console。该订阅为事件警告在事件过滤器中提供一个目标。您可以订阅或取消事件警告，以确定希望哪些设备警告显示在 HPCA Console 中。

Intel vPro 设备在其固件芯片中内置了一组默认事件过滤器。 HPCA Console 还允许在事件日志中查看特定 vPro 设备的事件，以确定每个记录的事件的类型、严重性、日期和描述。

您可以使用此功能控制事件警告和日志记录。发送到控制台的警告和写入事件日志的事件可用于确定特定设备是需要修复还是保护操作。

保护

您可以保护网络上的 vPro 设备，使其免受恶意软件攻击和蠕虫病毒繁殖。Intel vPro 通过过滤数据包和监视网络设备上是否存在运行中的关键 OOBM 代理程序来实现此功能。它还提供持续观察传出流量以检测和阻止蠕虫病毒繁殖的机制，从而使您可以隔离感染蠕虫病毒的设备。

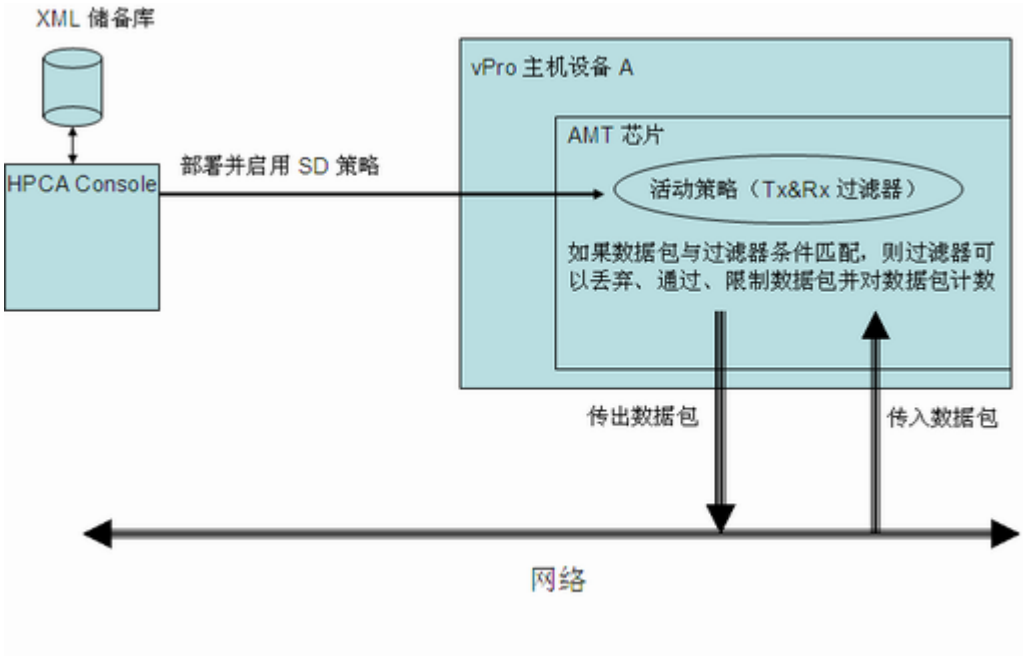
下面各节分别对这些主题进行了说明：

- 系统防御
- 代理程序存在
- 启发式网络病毒爆发控制

系统防御

下图显示了系统防御的大致工作原理，它使用策略和过滤器来监视通过 vPro 设备传输或接收的数据包。

图 5　系统防御概述



策略

系统防御 vPro 功能允许 HPCA Console 定义和执行网络安全策略。系统防御策略包含一组应用于传入和传出网络数据包的过滤器，以及数据包与过滤器中的条件匹配（或不匹配）时应采取的操作。系统防御允许您根据与策略关联的过滤器对 Ethernet 和 IP 协议流量进行选择性的网络隔离。这些过滤器允许管理控制台通过、限制或阻止基于特定 IP 的网络流量，保持流量计数或记录这些流量的发生。

HPCA Console 将这些过滤器和策略存储在 XML 储备库中。然后控制台就可以将系统防御策略部署到它们驻留在其固件上的多台 vPro 设备。

将策略部署到 vPro 设备后，可以通过 HPCA Console 使该设备上的策略成为默认系统防御策略。另外，还可以将策略设置为监视程序操作可启用的代理程序存在策略。这方面的内容将在代理程序存在（第 172 页）中再作详细介绍。已启用的优先级更高的策略将成为设备的活动策略。策略激活后，vPro 设备会检查每个传入和传出数据包，必要时会执行由与策略关联的过滤器指定的操作。如果 vPro 设备具有多个网络接口卡 (NIC)，即有线和无线接口卡，则可以启用系统防御策略，并为每个 NIC 设置代理程序存在策略。

过滤器

如果符合与过滤器关联的条件，则过滤器可以执行以下操作：

- 通过数据包
- 丢弃数据包
- 限制数据包
- 对数据包计数以收集统计数据

除执行与数据包相关的操作外，过滤器还可以引发事件。

有两种过滤器模式。它们分别是：

- **传输**：此模式的过滤器适用于从 vPro 设备传输到网络的数据包。这类过滤器可用于阻止疑似感染病毒的设备的所有流量，防止它感染网络上的其他设备。传输模式的默认过滤器会捕获所有与任何其他策略传输过滤器都不匹配的传输数据包。此模式的过滤器类型可以是通过、限制、统计或丢弃。
- **接收**：此模式的过滤器适用于从网络接收到 vPro 设备的数据包。这类过滤器可用于阻止设备从引导后到 OOBM 代理程序启动 （比如防病毒代理程序）为止所接收的所有数据包。接收模式的默认过滤器会捕获所有与任何其他策略接收过滤器都不匹配的接收数据包。此模式的过滤器类型可以是通过或丢弃。

有多种过滤器类型。它们分别是：

- **默认否则**：是接收和传输方向模式的默认否则过滤器，用于捕获所有与任何策略过滤器的条件都不匹配的数据包。如果与否则过滤器匹配，也就是说数据包与所有其他过滤器都不匹配，则可以生成过滤器操作。
- **丢弃**：是接收和传输方向模式的丢弃过滤器，丢弃所有与该过滤器条件匹配的数据包。
- **通过**：是接收和传输方向模式的通过过滤器，通过所有与该过滤器条件匹配的数据包。

- **统计丢弃 / 通过**：是接收和传输方向模式的统计过滤器，计算与相应过滤器条件匹配的数据包数目，用于收集统计数据。统计过滤器可以根据它们是统计通过还是统计丢弃过滤器，从而通过或丢弃数据包。
- **速率限制**：是接收和传输方向模式的速率限制过滤器，限制每秒钟接收或传输符合过滤器条件的特定类型数据包的数目。此过滤器有阈值，达到阈值时就中断所有其他流量。

除过滤器类型外，传输过滤器还可以启用防欺诈属性。启用此属性后，所有传出数据包都要经过检查，且源 IP 要与网络接口 IP 地址进行比较。如果 IP 地址不匹配，则丢弃数据包。如果启用了此过滤器，它可防止主机用非分配的 IP 地址的源 IP 地址发送 IP 数据包来伪造其身份。

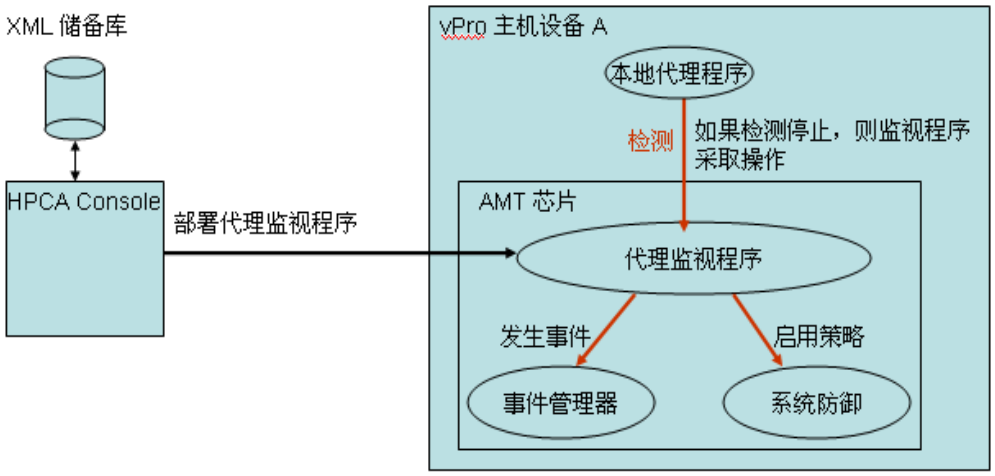
Intel vPro 支持 32 个接收 (Rx) 模式的过滤器和 32 个传输 (Tx) 模式的过滤器。 32 个 Tx 和 32 个 Rx 模式中的每个过滤器都用作 “否则”（不匹配）过滤器。如果启用防欺诈，它使用 Tx 模式中的某个过滤器。这会使 vPro 设备的可用过滤器减少到 31 个入站和 30 个出站过滤器。

如果达到此限制，则只有在删除该设备上的一部分现有过滤器后，才能将包含过滤器的其他策略部署到 vPro 设备。

代理程序存在

下图显示了监视 vPro 主机设备上是否存在 OOBM 代理程序所涉及的组件。

图 6　代理程序存在概述



代理程序存在功能允许 HPCA Console 创建监视程序，监视 vPro 设备的主机 CPU 上运行的 OOBM 代理程序状态。 OOBM 代理程序通常是通过监视与防病毒或防火墙保护相关的安全应用程序来保护 vPro 设备的软件。启动后， OOBM 代理程序定期将检测信号发送到监视程序。如果检测信号停止，监视程序将采取操作来保护设备。

OOBM 代理程序

如上所述，OOBM 代理程序通过监视 vPro 设备上运行的任何关键应用程序的状态，从而保护设备安全。 OOBM 代理程序所监视的应用程序列表由用户定义。如果受监视的应用程序停止运行，OOBM 代理程序会停止向监视程序发送检测信号。如果监视程序启用代理程序存在策略，且该策略成为活动策略，则在 vPro 设备的控制台上显示系统消息。尽管提供默认消息，但系统消息也是用户定义的。应用程序列表和系统消息都存储在 vPro 设备的 3PDS 中。

当 OOBM 代理程序安装完成 （应用程序软件列表创建好并部署到设备）后，它会自动作为 NT 服务启动。启动后， OOBM 代理程序执行以下操作：

1. 向监视程序注册。
2. 从 vPro 芯片获取检测间隔，并开始将检测信号发送到监视程序。
3. 读取 3PDS 数据以获取要监视的应用程序列表，并开始监视应用程序。使用相同的检测间隔监视应用程序列表。
4. 如果应用程序列表上的某个应用程序停止运行，则停止发送检测信号。
5. 关闭监视程序，并显示从 3PDS 读取的用户定义的系统消息。

监视程序

监视程序可以执行如下操作：

- 启用代理程序存在策略 （如已设置） 。如果代理程序存在策略的优先级比默认的系统防御策略高，前者将成为活动策略，且激活与此策略关联的过滤器来保护网络。
- 发起事件。根据事件管理器在事件过滤器中发现的信息，将事件写入 vPro 芯片的事件日志，和 / 或将事件警告发送给 HPCA Console （如已订阅）。

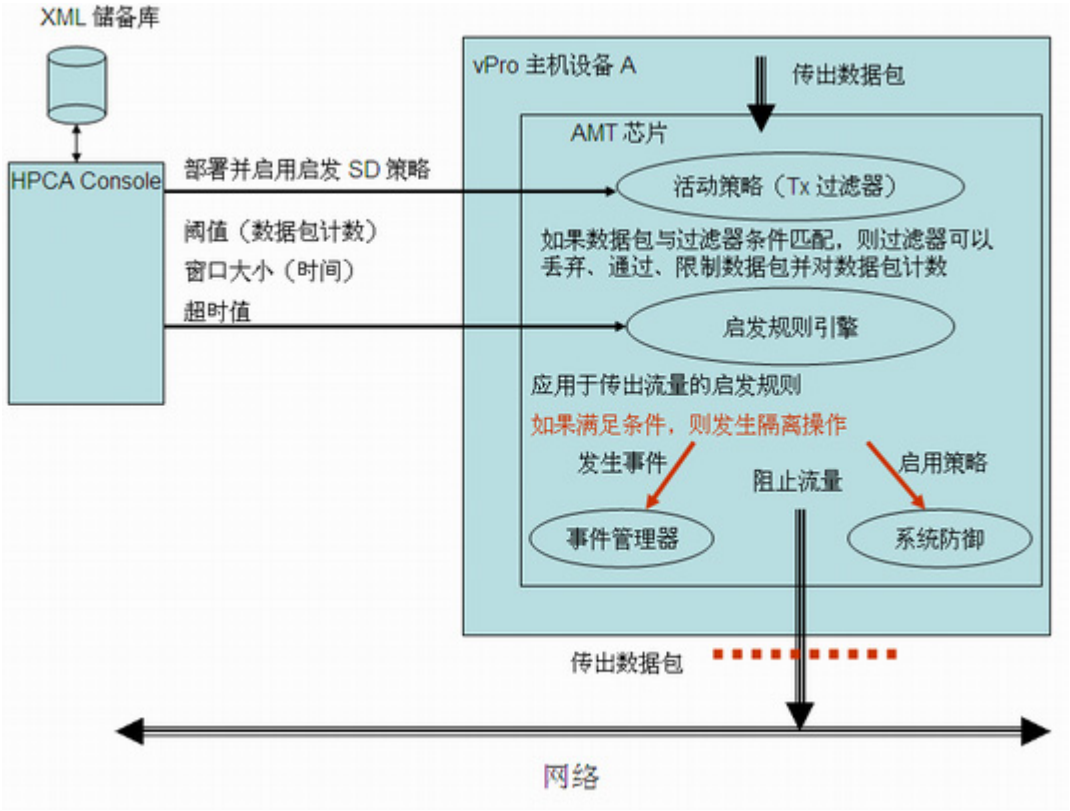
您可以使用 HPCA Console 执行以下操作：

- 创建监视程序。
- 指定计时器，检测 OOBM 代理程序初始化和定期将检测信号传输到其监视程序的时间。
- 指定将触发监视程序操作的 OOBM 代理程序的转换状态。有效状态包括：
  - 未启动
  - 已停止
  - 正在运行
  - 已过期
  - 已挂起
- 设置监视程序在满足转换条件时要采取的操作（即，启用代理程序存在策略和 / 或启用事件日志记录）。
- 在多个 vPro 设备上部署 （和取消部署）监视程序。
- 创建 OOBM 代理程序要监视的应用程序列表。
- 创建激活代理程序存在策略时要显示的消息。

启发式网络病毒爆发控制

下图是蠕虫病毒控制系统的体系结构概述。

图 7　蠕虫病毒控制系统体系结构



即便网络中有防火墙和入侵检测系统，启发式蠕虫病毒控制机制也可以为网络提供附加价值。防火墙和入侵检测系统只针对已知蠕虫病毒，而不能有效阻止零日蠕虫病毒爆发。

vPro 蠕虫病毒控制系统是通过将启发式规则应用于主机 vPro 设备的出站流量而起作用的。如果启发式规则引擎检测到异常，则蠕虫病毒控制系统会将主机从网络中隔离出来。活动策略过滤器过滤主机流量的 IP 和 TCP/UDP 协议报头字段。过滤的结果是， vPro 芯片可能会采取特定操作，比如丢弃数据包。

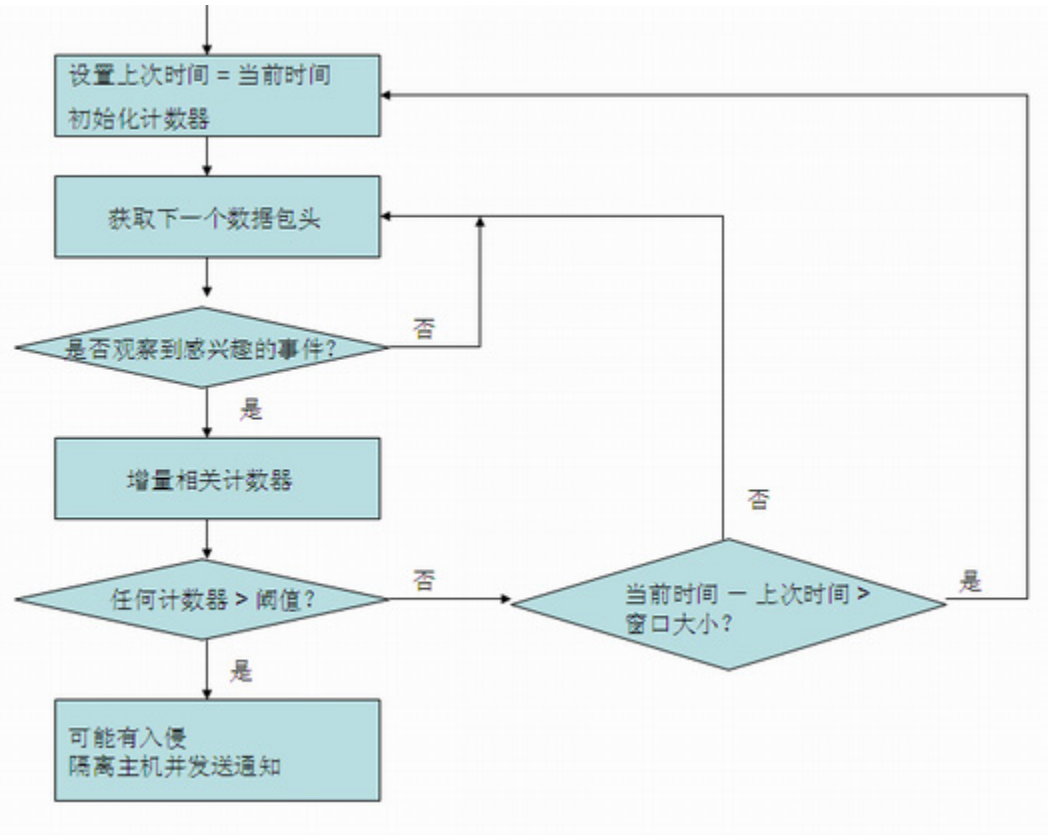
启发式规则引擎分析流量。如果启发式规则引擎检测到异常流量的情况，它可以执行以下任何一种操作：

- 引发事件警告。
- 引发事件警告，并阻止来自有问题端口的所有出站数据包。
- 引发事件警告，并阻止来自所有端口的所有出站数据包。
- 引发事件，并启用 vPro 系统防御策略。

蠕虫病毒控制系统依赖于启发式规则，来检测可能指示蠕虫病毒扫描活动的流量异常情况。启发式规则基于所有自我传播蠕虫病毒的基本属性，即，蠕虫必须联系新主机才能将病毒传播到网络上。因此，所有启发式规则都识别预示着与新主机联系的事件，并监视这些事件是否存在异常模式。

下图显示了所有启发采用的基本机制。

图 8　基本的启发操作



有关详细信息，请参见 Intel 对启发式蠕虫病毒控制系统的研究。

窗口大小和阈值

所有启发都会检查数据包报头，并计算一定时间间隔内 “感兴趣事件” 的数目。因此，所有启发都公开两项可配置参数，即窗口大小和阈值。窗口大小 （时间计数）表示启发重置其计数器的时间期间。阈值 （数据包计数）是一个限制值，当计数器超过此值时，表明有异常事件。

HPCA Console 允许您配置这两个参数。指定这些参数时，必须考虑两种类型的蠕虫病毒，它们需要不同的启发值。它们是快速传播蠕虫病毒和慢速传播蠕虫病毒。快速传播和慢速传播蠕虫病毒应使用不同的窗口大小和阈值，才能成功检测到蠕虫病毒感染。采用组合启发 （不同的窗口大小和适当的阈值），对蠕虫病毒的作用范围更广、更有效。启发的窗口大小越小，对快速蠕虫病毒越有效，启发的窗口大小越大，则对慢速蠕虫病毒越有效。

快速和慢速蠕虫病毒的可配置时间窗口大小范围如下：

- 快速：10 毫秒到 1 秒 （1000 毫秒）
- 慢速：1 秒 （1000 毫秒）到 50 秒 （50000 毫秒）

两种启发的可配置阈值范围都是 8 到 64 个数据包。

HP 建议将窗口大小和阈值组合配置如下：

- 快速：10 毫秒 8 个数据包
- 慢速：50 秒 64 个数据包

控制操作和超时值

如果超过阈值，则 HPCA Console 还允许指定系统应当采取的自发操作。如第 174 页所示，可以选择仅引发事件，也可以选择引发事件并结合阻止出站主机流量或启用启发式系统防御策略。采取操作后，启发式规则引擎将处于禁用状态。

您可以指定通过 HPCA Console 应用于 vPro 设备的控制操作应当持续多久。如果指定非零超时值（大于或等于 20 秒），则启发式规则引擎在该时间段停止扫描数据包并应用指定操作。经过该时间段后，操作将自动删除，芯片开始重新扫描数据包。如果指定零超时值，则启发式规则引擎永久停止扫描数据包并应用操作。要删除控制操作并重新开始扫描数据包，则必须通过 HPCA Console 手动触发这一操作。

B vPro 设备的延迟远程配置

当 vPro 设备无法在连接到网络之后网络接口打开的有限网络访问时间段内进行置备时，执行*延迟配置*。

本节涵盖以下主题：

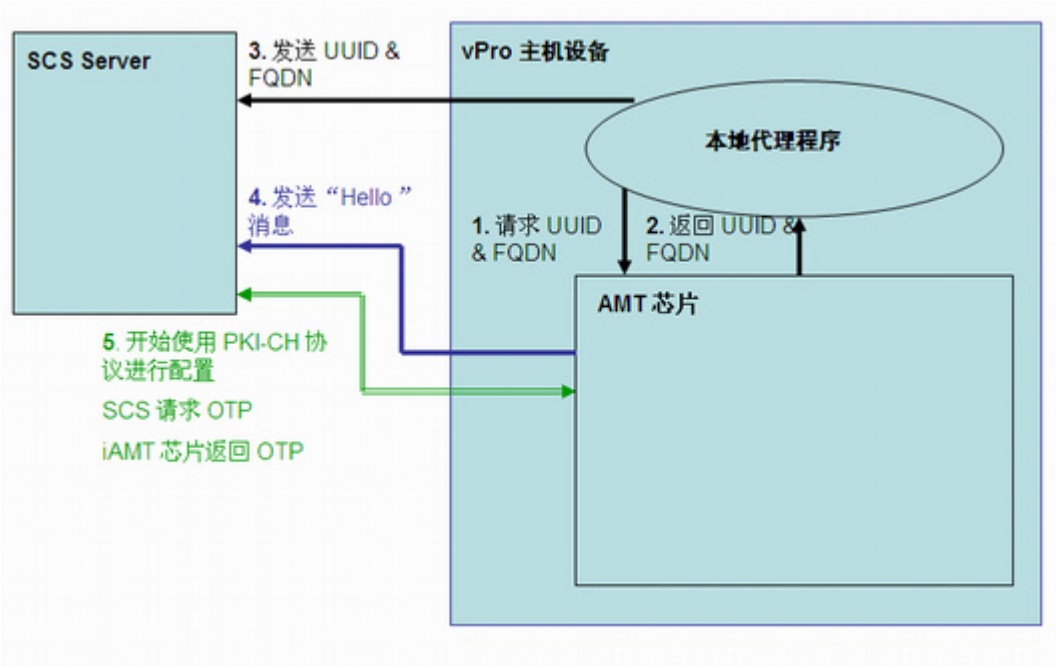
- 转换为设置模式
- 远程配置置备过程
- 通过 HPCA Console 的延迟远程配置

转换为设置模式

以下图表显示了在使用 OOBM 代理程序进行远程配置时将 vPro 设备转换为设置模式所涉及的步骤。之所以称为*延迟*配置是因为设备没有在连接到网络后立即进行置备。要了解对此备用（即时）配置的说明，请参见 vPro 设备的裸机远程配置（第 25 页）。

在 vPro 设备转换为设置模式后，它开始将 “Hello” 消息发送到 SCS Server，以指示准备好供置备。

图 9　在延迟配置中转换为设置模式



必须在 vPro 主机设备上安装 OOBM 代理程序。 OOBM 代理程序检测 vPro 设备，并发生以下操作：

1 OOBM 代理程序向 vPro 设备请求 UUID 和 FQDN。

2 vPro 设备将这些值返回给 OOBM 代理程序。

3 OOBM 代理程序将这些值发送到 SCS Server。

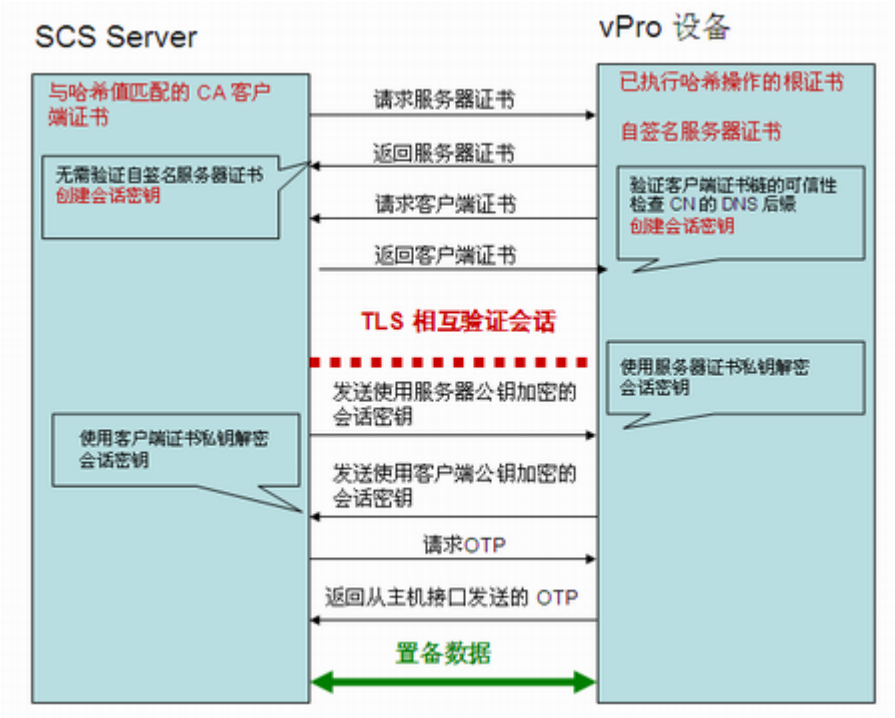
4 vPro 设备开始将 “Hello” 消息发送到 SCS Server。

5 SCS Server 使用 PKI-CH 协议启动置备过程。在 SCS Server 和 vPro 设备之间交换 OTP。

远程配置置备过程

在远程配置置备过程期间，通过使用 TLS 相互验证创建安全通道。以下图表演示置备过程流程。

图 10　远程配置置备过程



置备过程包括以下步骤：

1 OOBM 代理程序请求 vPro 设备启动配置过程。设备在一段有限的时间内打开其网络接口 （在 Intel 计算机上为 24 小时，在 HP 台式机上为 255 小时）并且开始发送 “Hello” 消息。首次启用 OOBM 时，接口在指定的小时数打开。如果在设置与配置完成之前超时，则要启动配置的 OOBM 代理程序的任何后续调用将仅打开端口六个小时。

2 SCS Server 执行以下操作：

— 从 “Hello” 消息中提取根证书哈希值，以了解向 vPro 设备发送何种客户端证书进行验证。

— 发送证书链，其中包括与已接收哈希值之一匹配的可信根证书。

3 vPro 设备执行以下操作：

— 验证 SCS 客户端证书。它检查 OID 或 OU 是否正确以及证书是否派生自与根证书哈希值之一匹配的 CA。

— 验证域后缀是否与 SCS 证书上的 DNS 后缀匹配。

4 SCS Server 和 vPro 设备执行完整的相互验证会话密钥交换。

— vPro 设备使用自签名证书，发送其公钥。

— SCS 创建 TLS 会话密钥、使用 vPro 设备公钥对其加密并将其发送到 vPro 设备。

— vPro 设备使用其私钥解密会话密钥。 vPro 设备创建另一个会话密钥，并使用 SCS Server 发送到该 vPro 设备以供验证的客户端公钥对该会话密钥进行加密。会话密钥对用于在安装和配置 TLS 会话期间对流量进行对称加密。

5 在 SCS Server 和 vPro 设备之间进行一次性密码 (OTP) 验证。 SCS Server 向 vPro 设备请求 OTP。设备安全地发送 OTP，并且 SCS Server 检查它是否正确。

6 在置备设备之前，安装和配置过程继续。由于 vPro 设备网络接口发送第一条 “Hello” 消息之后在一段有限的时间内打开，因此 SCS Server 可以指定 vPro 设备将此时间段延长最多 24 小时，以便完成配置过程。

通过 HPCA Console 的延迟远程配置

通过 HPCA Console，可以置备未在初始设置与配置服务 (SCS) 置备过程中置备的 vPro 设备。

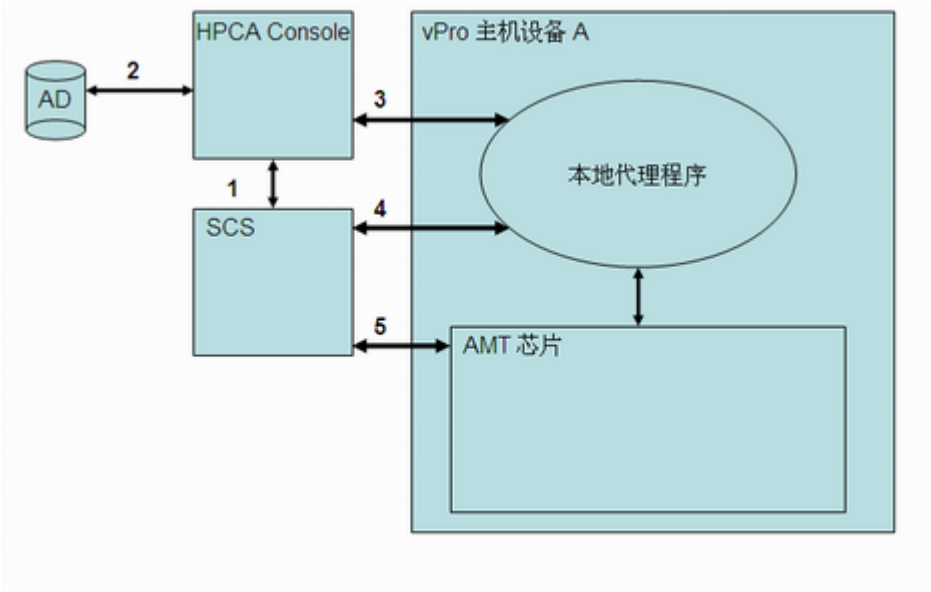
通过 HPCA Console 执行的置备类型称为延迟远程配置置备。之所以称为*远程*配置是因为您不必为使每台设备启用安装程序而手动安装 PID/PPS 对或输入有关 SCS Server 地址和域名等信息。可改为从管理控制台自动地、远程地完成此置备。之所以称为*延迟*配置是因为未在该设备初始连接到网络时的允许时间间隔内置备设备。

为了使用远程配置，必须遵循使用远程配置配置 vPro 设备 （第 24 页）所讨论的所有要求。

仅当 vPro 设备处于未置备或置备中状态时，可以使用远程配置来置备 vPro 设备。已置备的 vPro 设备无法再次使用远程配置进行置备。必须手动重新置备 vPro 设备。

为获取置备 vPro 设备的必需信息， HPCA Console 会与在 vPro 设备、 SCS Server 和 Active Directory 上运行的 OOBM 代理程序通信。

图 11　通过 **HPCA Console** 的延迟远程配置



通信交换如下：

1. HPCA Console 与 SCS 通信以获取已置备设备和当前置备中的设备的列表。
2. HPCA Console 与 Active Directory (AD) 通信以获取该特定域中设备的列表。管理控制台列出所有设备及其相应的置备状态。
3. HPCA Console 尝试在默认端口上与 OOBM 代理程序通信。如果安装了代理程序，则在 HPCA Console 中显示状态为未置备的设备。一旦与 OOBM 代理程序建立通信，则 HPCA Console 请求 OOBM 代理程序启动延迟的配置过程。
4. 如果设备未置备或处于置备中状态，则 OOBM 代理程序尝试与 SCS Server 联系以存储设备的 FQDN、 UUID 和配置文件标识。然后生成 hello 数据包。
5. SCS Server 使用 PKI-CH 协议置备 vPro 设备。

C 可信证书

可信证书

通过使用公钥基础结构 (PKI)，可以保护安全套接字层 (SSL) 连接。在 PKI 中，使用具有非对称密钥对 （公用和私用）的证书保护通信。客户端和服务器相互通信时，使用密钥对将交换的数据进行加密和解密。公钥是共享的，并且用于对数据加密。私钥由证书的所有者私人持有，并且用于对使用证书公钥加密的数据解密。

在服务器验证过程中使用 PKI 时，客户端使用服务器证书的公钥对消息加密，并且服务器使用其私钥对消息解密。反过来，在客户端验证过程中，服务器使用客户端证书的公钥对消息加密，并且客户端使用其私钥对消息解密。

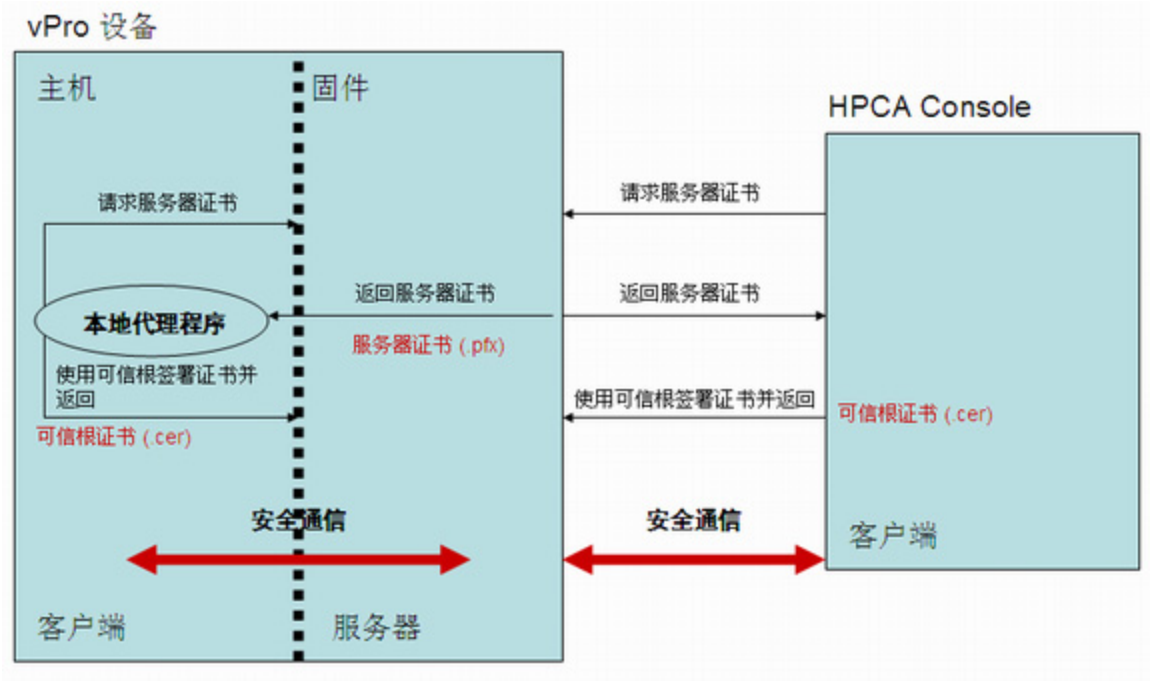
传输层安全 (TLS) 协议具有两类验证：TLS 服务器验证 （单向验证）和 TLS 相互验证 （双向验证）。在 TLS 协议中， vPro 设备上的固件是 SSL 服务器。 HPCA Console 和 / 或主机 vPro 设备上运行的 OOBM 代理程序充当客户端。

TLS 服务器验证

在 TLS 服务器验证过程中建立 TLS 会话时，客户端尝试验证它从 vPro 设备上的固件接收的 SSL 证书的有效性。要执行此验证，客户端必须具有签署该证书的证书颁发机构 (CA) 的公钥。公钥在由创建服务器证书的相同 CA 创建的可信根证书中可用。在连接到域的 Active Directory 的所有 vPro 系统上已填充可信根证书。客户端使用验证服务器身份的可信根证书签署证书，并将其发送回服务器。这可以在客户端将应用程序数据发送到固件时，保护充当客户端的组件和 vPro 设备的固件之间的通信。

在以下图表中，在主机设备上运行的 OOBM 代理程序和 HPCA Console 都是指向 vPro 固件的客户端。 OOBM 代理程序的功能随后将在本章以及本指南中进行更加详细的讨论。

图 12　TLS 服务器验证



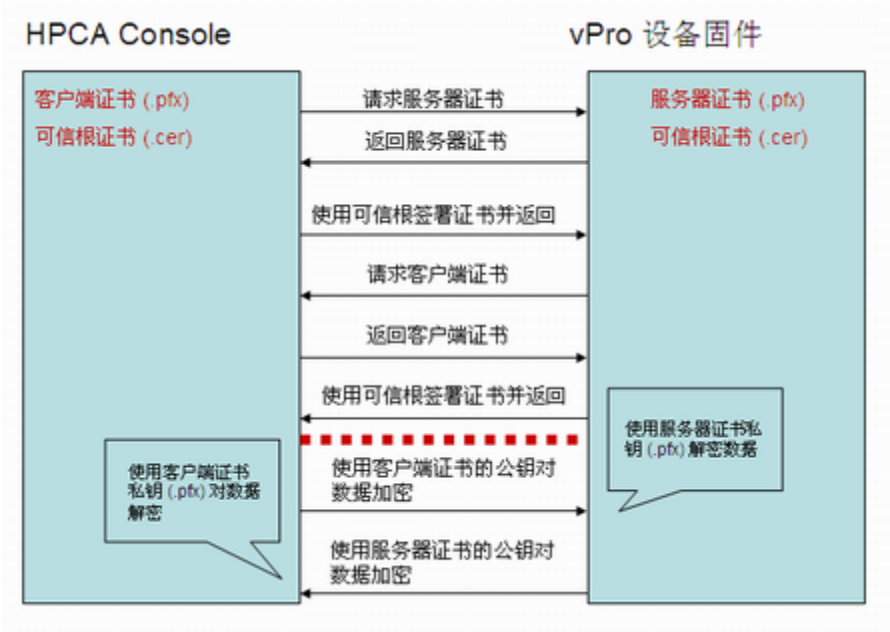
TLS 相互验证

除了在客户端和服务器之间仅传递一个证书的 TLS 服务器验证以外， TLS 相互验证可以提供更高的安全，因为它会传递两个证书以验证通信的两端。在相互验证中，客户端发送必须由服务器签署的证书，同时服务器发送由客户端签署的证书。如前所述，使用证书的公钥和私钥进行数据的加密和解密。

在此模型中， HPCA Console 和 / 或 OOBM 代理程序再次充当 SSL 客户端。客户端必须将自己的 SSL 客户端证书发送到 vPro 设备以进行客户端验证，并且 vPro 设备必须将可信根证书 （公钥）导入其固件中以执行验证 （签署客户端证书）。

HPCA Console 是客户端时，可信根证书还必须导入到 HPCA Console 计算机上的可信密钥库中。这允许 HPCA Console 签署 vPro 设备发送给它以验证服务器的服务器证书。在 HPCA Console 上安装的客户端证书必须包含完整证书链以及证书的私钥。此功能提供了客户端和服务器的相互验证，增加了 TLS 会话的安全级别。在以下图表中， HPCA Console 正在充当指向 vPro 固件的客户端。

图 13　HPCA Console 和 vPro 设备固件之间的 TLS 相互验证



指定 vPro 客户端证书时，存在某些要求。它们包括以下内容：

- 证书必须包含将其标记为 TLS 证书的 1.3.6.1.5.5.7.3.2 OID。
- 叶子证书的增强型密钥使用 OID 列表字段必须包含 2.16.840.1.113741.1.2.1 OID。 vPro 设备使用此 OID 验证 HPCA Console。

在创建服务器和客户端证书模板的过程中将使用这些值。要使用相互验证功能，vPro 设备必须具有签署其可信列表中的 SSL 客户端证书的根证书。在设置与配置过程期间将根证书提供给 vPro 设备。这在创建和配置配置文件 （第 22 页）中进行了描述。